UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA UNIVERSITARIA DE INGENIERÍA TÉCNICA DE TELECOMUNICACIÓN

Proyecto Fin de Carrera

Sistemas de pago emergentes con móvil

Autor
Félix Suárez Camiño

Tutora
Ana Gómez Oliva

Noviembre 2012

Tema: Comercio electrónico y sistemas móviles

Título: Sistemas de pago emergentes con móvil

Autor: Félix Suárez Camiño

Tutor: Ana Gómez Oliva

Departamento: Diatel

Presidente: Javier Malo Gómez

Vocal: Ana Gómez Oliva

Vocal Secretario: Emilia Pérez Belleboni

Fecha de lectura: 27/11/2012

Resumen

Los sistemas de pago con móvil son una alternativa de pago a los medios de pago electrónicos tradicionales que están siendo cada vez más utilizados en nuestra sociedad.

Son varios los factores que han llevado a la utilización de esta forma alternativa de pago. Los terminales móviles se han convertido en una herramienta casi vital para la sociedad, lo cual ha contribuido a una gran aceptación y desarrollo de los terminales móviles que cada vez cuentan con más funcionalidades. Gracias a esto, las comunicaciones móviles también están en constante evolución y ello ha influido notablemente para que se puedan desarrollar nuevos servicios e implementar nuevas funcionalidades en los terminales móviles.

Por otro lado, la tendencia de los usuarios a usar cada día más los sistemas de pago electrónicos, intentando en la medida de lo posible prescindir del dinero en efectivo, también es un factor que ha permitido impulsar el desarrollo de este tipo de sistema de pagos emergentes.

En el otro lado se encuentra el mundo empresarial, donde por un lado están las empresas de telecomunicaciones que no quieren dejar escapar esta oportunidad de negocio y están invirtiendo dinero para desarrollar nuevas infraestructuras que permitan el pago con móvil, y por otro lado se encuentran las entidades financieras que son necesarias para poder llevar a cabo los pagos a través del móvil, y por tanto tienen que formar parte de la solución llegando a los acuerdos necesarios con los proveedores de servicios.

En este trabajo se realiza un análisis de las diferentes plataformas de pago por móvil existentes en la actualidad, prestando especial atención a los aspectos que tienen que ver con la seguridad y la disponibilidad y acceso

de la información bancaria del usuario. Asimismo también se analiza la arquitectura de cada plataforma como su funcionamiento, aclarando la interacción y el papel que juegan las diferentes partes implicadas.
Para ello hay un capítulo dedicado a la seguridad donde se presentan conceptos y protocolos que son aplicados en las soluciones de pagos electrónicos, y una descripción de los sistemas de pago electrónicos más usados actualmente, los cuales presentan muchas similitudes con los sistemas de pago con móvil.

Por último se recogen diferentes experiencias llevadas a cabo en nuestro país de pagos con móvil, destacando la experiencia de los usuarios así como el método empleado.

Abstract

Mobile payment systems are payment methods alternative to traditional electronic payment ones that are being increasingly used in our society. Several factors have led to the use of this alternative form of payment. Mobile terminals have become almost a vital tool for society, which has contributed to a wide acceptance and development of mobile terminals that are getting more features all the time. As a result, mobile communications are also evolving and they have had such a great influence that they have developed new services and implemented new features in mobile terminals. What is more, the growing tendency among users to use electronic payment systems, trying to make their payments whithout cash as often as possible, is also a factor that has allowed the boost the development of such emerging payment systems.

The other partner of these systems is the business world, where on one hand, the telecommunication companies that do not want to miss this business opportunity are investing funds to develop new infrastructures which enable the mobile payment, and on the other hand, the financial institutions that are necessary to carry out payments via mobile, and therefore need to be part of the solution reaching the necessary agreements with service providers, want their own saying and their own share of the potential profits.

This report is an analysis of the different mobile payment platforms existing today, with particular attention to the aspects that have to do with security and the availability and acces of user's bank information. Likewise, it also analyzes the architecture of each platform and its operation and interaction procedures, clarifying the role of the different parties involved.

Previously there is a chapter that presents security concepts and protocols that are applied in electronic payment solutions, and a description of the electronic trade systems most widely used currently, which have many similarities with mobile payment systems.

Finally, it shows different experiments carried out in our country of mobile payments, highlighting the experience of users as well as the method used.

ÍNDICE

1.-INTRODUCCIÓN

Los pagos efectuados con terminal móvil se están convirtiendo hoy en día en una alternativa real a los métodos de pago tradicional y a los más que implantados métodos de pago con tarjeta. Cada vez son más las empresas que están apostando por este tipo de soluciones y están favoreciendo el despliegue de este tipo de plataformas de pago.

Los factores que están impulsando este nuevo sistema de pago son diversos, y están relacionados con diferentes ámbitos. A continuación se tratará de enumerar los más importantes.

El teléfono móvil se ha convertido desde hace años en un objeto casi de primera necesidad del que todo el mundo hace uso a diario. Sumado a eso, existe una migración consolidada de terminales móviles hacia los smartphone, los cuales han experimentado un tremendo éxito entre los usuarios, especialmente en nuestro país, donde según un estudio realizado por la empresa Nielsen a finales de 2010, España ya ocupaba la segunda posición a nivel mundial en índice de penetración de smartphones, por detrás de Italia y por delante de países como Reino Unido, Estados Unidos, Alemania o China.

Los smartphones permiten el desarrollo de funciones muy avanzadas, la integración de nuevas tecnologías como el NFC, y manejar sistemas de cifrado muy robustos.

Además, por otro lado, existen una serie de “nuevas” tecnologías competitivas que han experimentado una maduración considerable, permitiendo la implantación de nuevas soluciones con garantías suficientes, como es el caso de los códigos de barras bidimensionales, lectores de banda magnética o Near Field Communication (NFC), las cuales permiten el desarrollo de diferentes soluciones de pago con móvil.

Por otra parte, las grandes empresas ligadas al mundo de las telecomunicaciones y del comercio electrónico no quieren dejar pasar

esta gran oportunidad de negocio que se les puede brindar, por lo que también están apostando por esta forma alternativa de pago aportando nuevas soluciones. Así, empresas como Google o Paypal ya han lanzado al mercado aplicaciones que permiten el pago con terminal móvil, y todo parece indicar que las empresas del sector invertirán y desarrollarán más aplicaciones relacionadas con la banca móvil. Asimismo, también instituciones públicas y empresas privadas, como por ejemplo el gobierno autonómico de La Comunidad Murciana o la empresa Movistar, están invirtiendo dinero en proyectos piloto que potencian el uso del móvil convirtiéndolo en un actor principal en tareas de identificación, integrando el DNI en el móvil, o la posibilidad de realizar el checkin en el aeropuerto, o también, poder utilizar el móvil como monedero electrónico para poder pagar el transporte público.

Otro de los factores decisivos que está propiciando el desarrollo de esta alternativa de pago es el factor sociológico. En muchas ocasiones a pesar de que las tecnologías están lo suficientemente maduradas y gozan del beneplácito y el acuerdo de todas las empresas implicadas en su puesta en marcha, puede que una solución determinada no triunfe porque no cuenta con la aprobación de los usuarios, o estos, en ese momento no encuentran la necesidad de hacer uso de la tecnología. De ahí el porqué de que muchas empresas inviertan enormes cantidades de dinero en marketing con el fin de generar una necesidad al usuario final. Pero eso es un factor que se desvía de este análisis.

En este caso, los usuarios ya han demostrado por un lado su preferencia por métodos de pago que no impliquen tener que llevar dinero en efectivo, ya sea por motivos de seguridad o de comodidad, y por otro, que la reticencia a utilizar métodos de pago electrónico sobre todo por motivos de seguridad ha ido desapareciendo, dado que confían cada vez más en los complejos mecanismos de seguridad que están desarrollados para llevar a cabo este tipo de transacciones.

Hay que tener en cuenta que diseñar un sistema de pago por móvil es una tarea muy complicada que implica a muchas partes, como por ejemplo, compañías telefónicas, identidades bancarias, fabricantes, etc, que se tienen que poner de acuerdo para solucionar problemas de estandarización, cuestiones legales, o problemas de entorno tecnológico. Pero en definitiva, todo apunta a que tras múltiples tentativas anteriores por impulsar este tipo de tecnologías que se vieron truncadas por diversos motivos indicados anteriormente, actualmente se dan las condiciones necesarias para que los sistemas de pago con móvil se consoliden como una alternativa de pago electrónico móvil, a pesar de las mejoras futuras que se puedan llevar a cabo en temas de usabilidad, costo y seguridad.

Por esta razón esta nueva forma de pago será objeto de estudio en este trabajo.

Primero haré una pequeña introducción situando el contexto tecnológico dónde se encuentran los sistemas de pago con móvil. Explicaré brevemente que es el comercio electrónico y en qué consiste, definiendo los diferentes tipos, los participantes y la manera de interactuar entre ellos.

Dado que la seguridad es un tema fundamental en cualquier sistema de pago, dedicaré un capítulo a explicar fundamentos de seguridad telemática que servirán de apoyo para poder entender con más facilidad los protocolos utilizados en los sistemas de pago electrónico y las nuevas soluciones que van surgiendo en este mundo de la seguridad en cuanto a pagos.

Después, antes de entrar de lleno en las plataformas de pago con móvil y las diferentes soluciones existentes, dedicaré un tema a los sistemas de pago electrónico ya existentes, aprovechando para explicar su funcionamiento, ya que en gran porcentaje se parece a los realizados con terminal móvil, sobre todo los que van asociados a una tarjeta de crédito, y servirá para tener una visión más general.

A continuación habrá un pequeño tema dedicado al terminal móvil como núcleo del sistema de pago que se presenta en este trabajo, explicando básicamente su estructura y las partes más importante que participan en las transacciones de pago.

Finalmente, se presentarán las diferentes soluciones de pago con móvil existentes, explicando su funcionamiento y arquitectura y destacando sus ventajas y desventajas.

Para terminar, se presentarán algunos casos de éxito y pruebas piloto realizas con sistemas de pago con móvil, se expondrán porcentajes de uso actuales y se realizará un pequeño análisis de la situación actual y futura de los pagos con móvil.

El trabajo se cerrará con un capítulo final de conclusiones personales.

2.-MARCO TECNOLÓGICO

El contexto dentro del cual se desenvuelven los sistemas de pago con móvil es el comercio electrónico. El comercio electrónico cuenta con una historia reciente y estrechamente ligada al mundo de las telecomunicaciones, puesto que ha sido internet en gran medida quien ha permitido su desarrollo. Por un lado la aparición de la tecnología www y su posterior evolución a la web 2.0, la aparición de nuevos lenguajes de programación como javascript o php que han contribuido al desarrollo de las tecnologías web, el avance en nuevos mecanismos y protocolos de seguridad, y una fuerte evolución en las redes de comunicación, tanto en los medios de transmisión hardware y nuevos protocolos de comunicación, han permitido el nacimiento y la proyección del comercio electrónico hasta nuestros días. De tal manera que hoy en día, casi todas las empresas tienen su propia página web que además de desempeñar un papel informativo y publicitario, permite la compra online de sus productos. Adicionalmente hay que decir que la consolidación del comercio electrónico ha contado con la indiscutible aceptación de los usuarios ya que aporta una serie de ventajas tales como; rapidez, comodidad o en muchos casos el abaratamiento de los precios.

2.1.-Tipos de comercio electrónico

Existen diversas definiciones sobre el comercio electrónico, pero se puede afirmar en líneas generales que el comercio electrónico (e-commerce) es un término genérico que engloba todas las actividades comerciales de compra y venta de productos o servicios, soportadas y publicitadas a través de redes de comunicación en lugar de utilizar la presencia física o directa.

Dentro del comercio electrónico podemos diferenciar varios tipos dependiendo de la naturaleza de las transacciones y quien se vea implicado en ellas. Los sistemas de pago por móvil se podrían clasificar principalmente dentro de dos tipos de comercio electrónico que se describen a continuación.

- ***Negocio a consumidor (B2C):*** se trata del modelo de negocio común, donde se produce un intercambio entre un negocio y un consumidor. Pero aquí el producto es ofrecido mediante una interfaz web. La principal ventaja de este modelo es la posibilidad de crear un vínculo directo con el cliente sin necesidad de que haya intermediarios. Se puede hacer una clasificación de las empresas que venden directamente por internet a sus consumidores.
  - ✓ De mercadeo directo: empresas manufactureras que venden sus productos directamente. En este caso las órdenes de compra son recogidas directamente de los consumidores y pasan directamente a la fábrica sin previo paso por ningún intermediario.
  - ✓ Tiendas no físicas: tiendas que solo ponen a la venta sus productos a través de los portales web y que pueden vender tanto productos físicos como productos digitales.

- ***m-commerce:*** se trata del modelo más reciente que está relacionado con la tendencia cada vez más extendida de la utilización de dispositivos móviles para conectarse a internet. A través de los dispositivos móviles y gracias a ciertas aplicaciones desarrolladas específicamente para el comercio electrónico, se puede hacer negocio a través de estos dispositivos. Actualmente representa una pequeña parte del total de transacciones que tienen lugar dentro del comercio electrónico, sin embargo sus ingresos

crecen a un ritmo constante. Destacan los servicios basados en localización y las aplicaciones B2C y C2C.

El marco en el cual se desarrollará este trabajo está relacionado con el modelo B2C, orientado sobre todo a usuarios domésticos, y por supuesto el modelo m-commerce, que permite realizar la compra del producto deseado desde el terminal móvil.

2.2.-Escenario común del comercio electrónico

Por tanto existen diferentes tipos de comercio electrónico, los cuales están perfectamente clasificados obedeciendo a la naturaleza de sus transacciones y cada tipo presenta unas características determinadas. Sin embargo, se puede describir un escenario general común a todos ellos, donde se puede observar el flujo de información que tiene lugar en una transacción de comercio electrónico, donde lo único que cambiaría sería la participación de ciertos actores. No hay que olvidar que la finalidad del comercio electrónico es la compra/venta de productos/servicios a través de internet.

Los participantes habituales en una transacción de comercio electrónico son:

El comprador: es la persona o entidad que va efectuar la compra del producto o servicio.

El comerciante: es la entidad que ofrece productos o servicios a cambio del pago.

Institución financiera: son las encargadas de materializar las transacciones y garantizar la solvencia del sistema.

En algunos casos existen actores adicionales que dependen del método de pago empleado, como en el caso de las tarjetas de crédito, donde las instituciones emisoras de tarjetas de crédito como visa o mastercard también participan en las transacciones.

En el caso de pagos realizados a través del teléfono móvil, las operadoras móviles también pasan a formar parte del escenario de pago cuando se trata de modelos no basados en bancos, y es la propia operadora móvil la que se encarga de la relación entre los clientes permitiéndoles a estos realizar transacciones de pago y transferencias de fondos siempre y cuando los usuarios se encuentren dentro de un mismo sistema.

A continuación se presenta el escenario que actualmente es más común y la interacción entre los diferentes participantes dentro de una transacción de comercio electrónico que se desarrolla de la siguiente manera.

El consumidor contacta con el comerciante a través de su página web, donde puede ver sus productos. Una vez el consumidor ha elegido el producto que desea comprar, el siguiente paso es introducir los datos necesarios para efectuar la compra (datos bancarios, cuenta de paypal…), en la web del comerciante para poder realizar la compra. Estos datos no pueden ser accedidos ni interceptados por nadie, ni siquiera por el comerciante. Por tanto aquí ya se plantea un primer problema de seguridad que hay que abordar con sumo cuidado. Esta comunicación normalmente tiene lugar a través de internet utilizando un protocolo muy común como es el http, que es fácilmente interceptable por cualquier usuario con unos conocimientos medianamente avanzados en telemática. Por tanto es esencial poder dotar a esta comunicación de una seguridad que permita garantizar la confidencialidad y la integridad los datos del consumidor. Para ello se utilizan una serie de protocolos que protegen cada nivel de la comunicación que tiene lugar, como https, SSL... los cuales se explicarán con más detalle en el capítulo de seguridad.

Una vez que el comerciante dispone de los datos necesarios para realizar la compra, normalmente valida estos datos con terceras partes de confianza, como por ejemplo la cámara de compensación o servidores de paypal. Esta tercera parte de confianza comprueba si los datos proporcionados son correctos y además se cercioran de que existen fondos suficientes para efectuar la compra. Nuevamente este paso es

crítico en cuanto a seguridad, porque la información no puede ser interceptada ni revelada por alguien no autorizado.

Para establecer estas conexiones entre comerciante y terceras partes de confianza, se pueden utilizar redes privadas virtuales (VPN), las cuales son capaces de simular una red privada y segura a través de una red pública como internet, utilizando técnicas de tunelado, autenticación y encriptación.

Si todos los datos son correctos, finalmente se realiza la transferencia correspondiente hacia el banco del comerciante. Para realizar la transferencia bancaria entre el banco del consumidor y del comerciante, los bancos utilizan sus redes privadas de valor añadido las cuales les ofrecen muchas más garantías de seguridad, ya que no pueden ser accedidas por cualquier usuario.

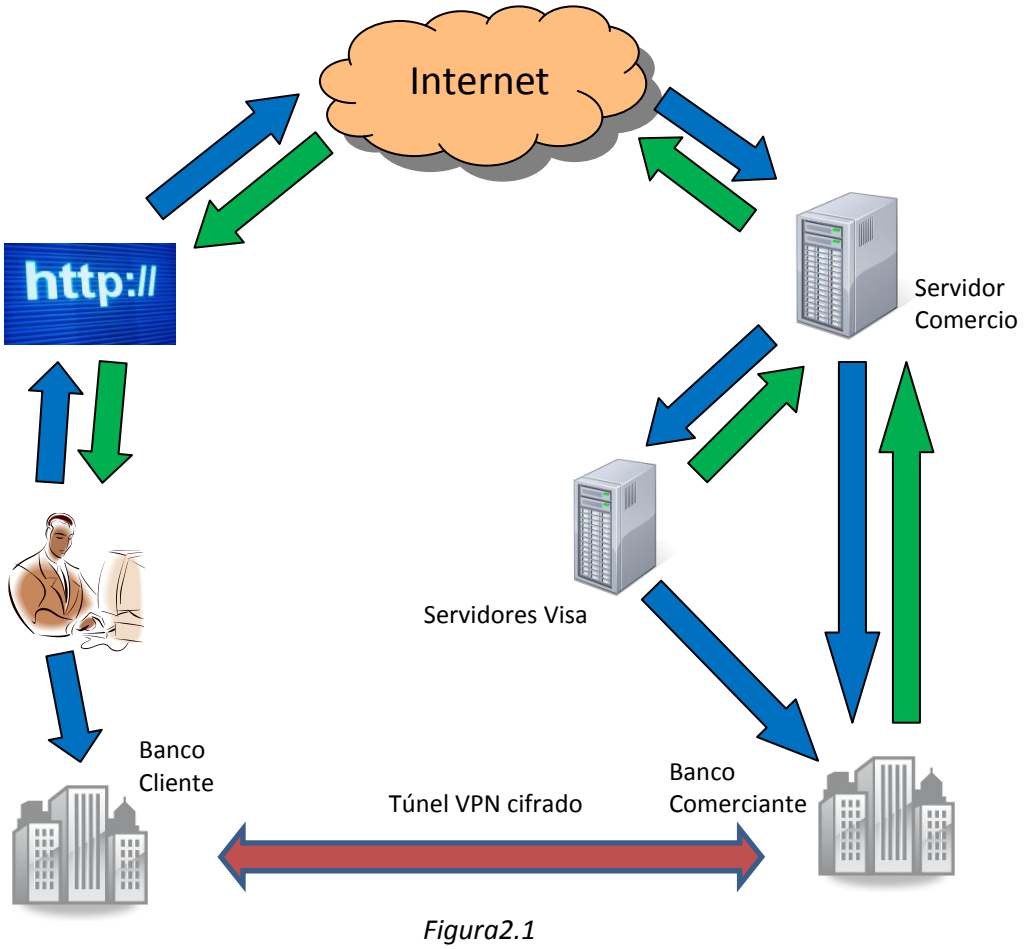

Figura2.1

Como se ha podido apreciar, en todo este proceso es fundamental la seguridad, ya que en las diferentes transacciones que tienen lugar durante la compra a través del comercio electrónico, existen distintas vulnerabilidades que hay que proteger.

Entre las vulnerabilidades más importantes se encuentran las amenazas de Sniffing, cuando tiene lugar la comunicación entre el consumidor y el comerciante, ya que cualquier usuario que tenga acceso al medio por el cual circula esa comunicación, es decir, internet, puede realizar ataques de alteración o robo de la información, denegación del servicio y robo o fraude en los servidores bancarios.

Estas amenazas de Sniffing todavía se acentúan más en el caso de los pagos con móvil, ya que a excepción de la tecnología NFC, que es de corto alcance, cuando accedemos a internet a través de nuestro móvil, lo hacemos vía radio utilizando las red PLMN (Public Land Mobile Network) y basta con que cualquier atacante esté escuchando en el medio electromagnético para poder capturar nuestros datos personales y bancarios, de ahí la importancia de la información vaya siempre encriptada.

Evidentemente, como se observa en el escenario descrito anteriormente, el comercio electrónico presenta características muy diferentes al comercio tradicional y hace necesario, por ejemplo entre otras cosas, la utilización de un método de pago diferente al pago tradicional, el pago electrónico.

El pago electrónico es un elemento esencial para el desarrollo del comercio electrónico. En la actualidad los sistemas de pago electrónico más utilizados son: tarjetas de crédito, monederos electrónicos (digital wallet), cheques electrónicos o sistemas que actúan como intermediarios del sistemas financiero como es el caso de PayPal.

Pero antes de continuar, debido a que la seguridad es un aspecto fundamental a tener en cuenta en las transacciones electrónicas, como

hemos podido observar, se detallarán algunos conceptos básicos relacionados con la seguridad de las redes de comunicación que serán de ayuda para entender posteriormente los protocolos y sistemas de comunicación utilizados.

3.-SEGURIDAD

Aunque como ya hemos visto, el comercio electrónico presenta ciertas ventajas, cuenta con un problema fundamental a la hora de realizar los pagos electrónicos, la seguridad.

Cuando realizamos un pago electrónico utilizando por ejemplo la tarjeta de crédito, nuestra información personal y bancaria circula a través de internet con el consiguiente riesgo que eso puede suponer, ya que un usuario que esté conectado a la red y realice una simple actividad de escucha de tráfico, puede conseguir nuestro nombre, nuestro número de cuenta y el código secreto asociado. No hay que olvidar que internet, por su propia naturaleza es abierto y de acceso libre a la información. Es por esto que la seguridad adquiere un papel esencial en este tipo de transacciones.

3.1.-Servicios de Seguridad

Dentro de la seguridad de las redes telemáticas existen una serie de servicios que se pueden proporcionar a las comunicaciones para proteger a estas frente a posibles ataques. Dentro del contexto de un pago electrónico existen tres de estos servicios que son fundamentales:

- *Autenticación:* este servicio sirve para verificar la identidad de los participantes en una comunicación, permitiendo garantizar a una entidad determinada que es quién dice ser.

- *Confidencialidad:* este servicio garantiza que la información no puede ser revelada por un usuario no autorizado.

- *Integridad:* este servicio garantiza que la información transmitida no ha sido alterada o destruida de manera accidental o deliberada.

- *Anonimato*: este servicio trata de mantener oculta la identidad de una entidad. Es uno de los servicios de seguridad más difíciles de proporcionar por la complejidad que entraña. El pago electrónico puede violar el derecho a la intimidad ya que quedan registros electrónicos que identifican al comprador, al vendedor, el importe, la fecha…etc, por eso es necesario este servicio.

Aunque existen más servicios de seguridad, estos se tornan los más importantes a la hora de realizar un pago electrónico.

Desde un punto de vista de comunicación estratificada en niveles, estos servicios son proporcionados desde una entidad N a la entidad N+1.

Para poder dotar de estos servicios a las comunicaciones, se tienen que implementar protocolos de seguridad, que definen un conjunto de reglas y formatos para el intercambio de piezas de información basándose en mecanismos de seguridad, cuya base principal es la criptografía. La siguiente figura ayudará al lector a comprender cómo se fundamenta un servicio de seguridad.

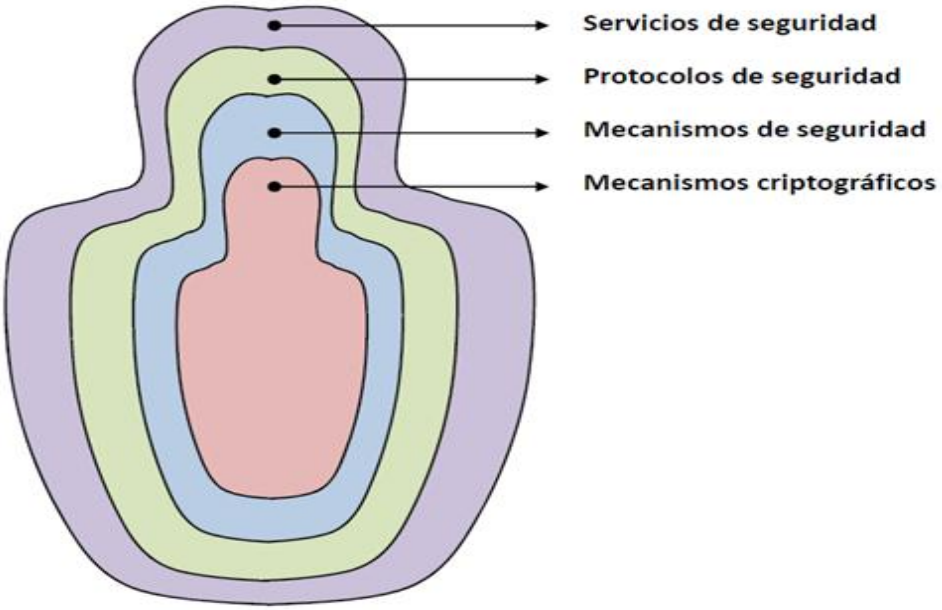

Figura 3.1

Por tanto, la criptografía es la base de la seguridad de las redes telemáticas en particular, y de las redes de telecomunicación en general.

La criptografía es la ciencia que trata de ocultar el contenido de un mensaje original (Kripto=ocultar, Graphos=escritura) utilizando diferentes códigos o algoritmos, pudiendo así, conservar mensajes seguros sobre canales inseguros.

Se trata de alguna forma de transformar un mensaje original de tal manera que no pueda ser entendible por cualquier persona que no disponga de una información secreta que le permita devolver el mensaje a su estado inicial. Esta información secreta es lo que se denomina clave, y es necesaria tanto para realizar la transformación inicial como para deshacer esa transformación.

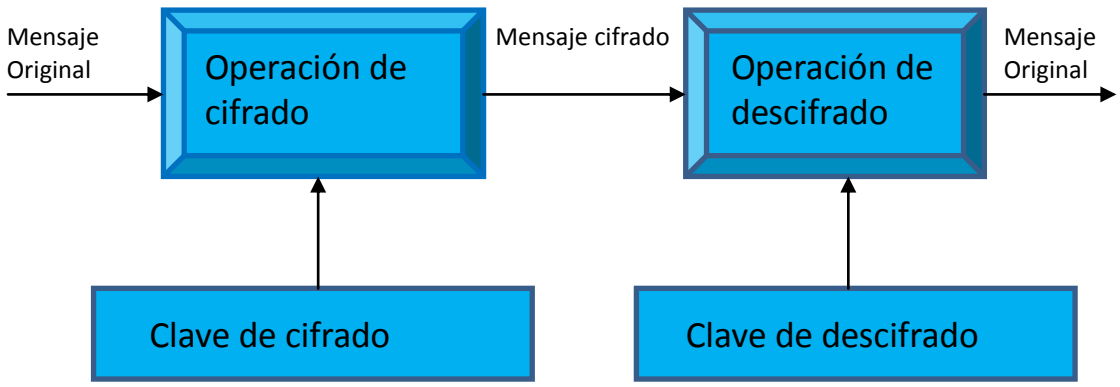

Figura 3.2

La complejidad de esta ciencia reside en desarrollar los algoritmos adecuados de cifrado y descifrado, y en encontrar un sistema seguro al mismo tiempo que eficaz para distribuir las claves que se aplican a los algoritmos, que son los que nos permiten hacer la transformación del mensaje para que no sea accesible por cualquier persona que no esté autorizada para poder ver ese mensaje.

3.2.-Criptografía

La criptografía moderna se empieza a considerar a partir de cuando aparecen los primeros algoritmos de encriptación diseñados para ser ejecutados sobre computadoras, allá por los años 70. Estos algoritmos tienen su base en operaciones matemáticas bastante complejas que con el tiempo han ido optimizando su ejecución gracias al avance que han sufrido los computadores en capacidad de procesamiento.

Otro de los rasgos de la criptografía moderna es que los algoritmos de encriptación son de conocimiento público. La fortaleza del sistema consiste en la ocultación de las claves y en la robustez del algoritmo de encriptación que se aplique.

Un buen algoritmo de encriptación es aquel que consigue que ante una pequeña modificación del mensaje en claro, el mensaje cifrado resultante sea totalmente diferente, dificultando así el criptoanálisis, que normalmente se fundamenta en la búsqueda de patrones basados en la entropía.

Los sistemas de cifrado en criptografía se conocen como criptosistemas, y un criptosistema se considera seguro cuando el tamaño de la clave de cifrado es igual al tamaño del mensaje en claro que se quiere cifrar. Un criptosistema muy seguro sería generar una clave aleatoria de igual tamaño al mensaje en claro, pero que solo sirva para una vez. La siguiente vez el algoritmo tendría que generar otra clave aleatoria. Este sistema se conoce como one-time pad.

En la criptografía moderna pueden distinguirse fundamentalmente dos tipos de criptosistemas:

✓ ***Criptosistemas de clave secreta o simétricos:***

Los criptosistemas de clave secreta utilizan un algoritmo conocido de encriptación, y se caracterizan porque tanto el emisor como el receptor del mensaje cifran y descifran utilizando la misma clave de seguridad.

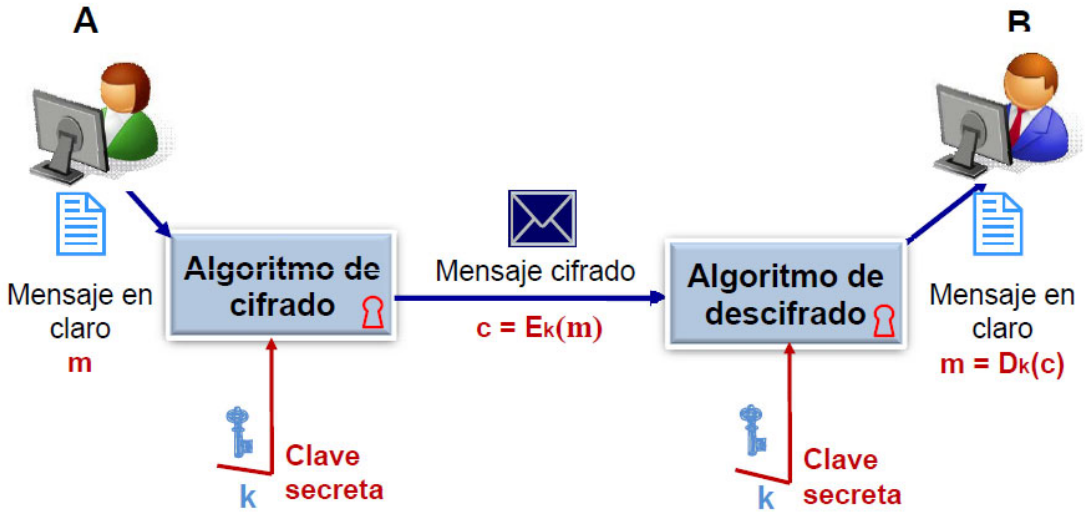

Figura 3.3

Donde k es la clave secreta, m el mensaje en claro, E_k representa la operación de cifrado del mensaje en claro, D_k representa la operación de descifrado del mensaje cifrado y c es el mensaje cifrado.

Estos criptosistemas son rápidos y fáciles de implementar, ya que sus algoritmos se basan en operaciones matemáticas no muy complejas de permutación y transposición. Esta característica hace que este tipo de algoritmos sean aplicables a comunicaciones telemáticas de gran velocidad, para proporcionar confidencialidad, debido a que se requiere gran rapidez en el flujo de datos.

Dentro de la criptografía simétrica existen fundamentalmente dos tipos de cifradores, que abordan básicamente la tarea de cómo dividir el mensaje

inicial en claro para proceder a su transformación y generar el mensaje cifrado, también conocido como criptograma.

- ***Cifradores de Flujo:***

Este cifrador consiste en ir cifrando bit a bit todos los bits que componen el mensaje en claro, con otra secuencia aleatoria de bits generada por un algoritmo determinístico de acuerdo a una clave secreta de tamaño predeterminado y no muy larga, mediante una operación lógica simple XOR.

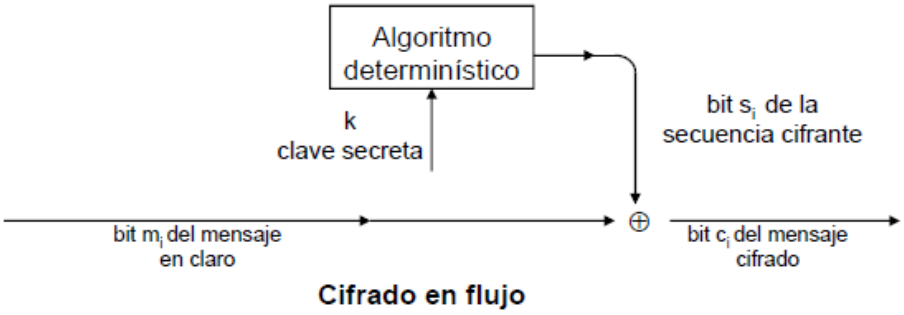

Figura 3.4

Ante una determinada clave k, el tamaño del mensaje cifrado siempre es igual a tamaño del mensaje original.

La gran ventaja de este criptosistema es que no se divide el mensaje inicial, por lo que gana en rapidez y además evita la necesidad de tener que usar buffers de memoria. En contrapartida es un es un sistema más débil en cuanto a seguridad se refiere y presenta algunas vulnerabilidades.

Un ejemplo muy significativo de este tipo de cifrado, es el utilizado por los usuarios de telefonía móvil en las redes GSM. Para proteger la comunicación desde la estación base hasta el terminal móvil, se utiliza un algoritmo de cifrado de flujo denominado A5. Este algoritmo permite una gran rapidez a la hora de cifrar la comunicación y sin la necesidad de disponer de ningún hardware adicional en el terminal móvil para llevar a

cabo este cifrado. Por contra, es un algoritmo que no es excesivamente fuerte y presenta debilidades que ya han sido vulneradas. Por eso cuenta con varias versiones, A5/1, A5/2 y A5/3.
En sus inicios el algoritmo A5 no era de dominio público y fue mantenido en secreto hasta que por técnicas de ingeniería inversa y gracias a sus debilidades pasó a ser de dominio público. Actualmente la versión que se utiliza es la A5/3 ya que es la más robusta. Las versiones A5/1 y A5/2 fueron reventadas.

- ***Cifradores de bloque:***

Los cifradores de bloque fraccionan el mensaje inicial en diferentes bloques del mismo tamaño que posteriormente se cifran por separado. A estos bloques se les aplica un algoritmo de cifrado con una clave secreta que ha de ser del mismo tamaño que los bloques para cumplir la condición de secreto seguro.

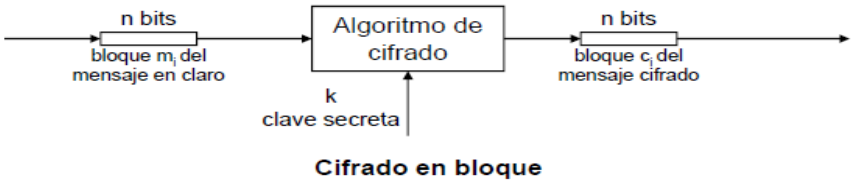

Figura 3.5

Este sistema de cifrado presenta la peculiaridad de que como el mensaje no tiene porqué ser múltiplo del tamaño de los bloques en los que ha sido dividido el mensaje inicial, estos bloques necesitan ser rellenados hasta alcanzar un tamaño (número de bits) múltiplo del mensaje en claro. A este relleno se le conoce como padding y está regulado por la PKCS#5. PKCS son las siglas de Public Key Cryptography Standars, y comprende un grupo

de estándares sobre criptografía que fueron publicados por los laboratorios RSA.

Hay que destacar que por motivos de seguridad, aun cuando el tamaño del bloque es múltiplo del mensaje original, se realiza padding igualmente por lo que el tamaño del mensaje cifrado siempre será mayor que el del mensaje original.

En general los cifradores de bloque son más seguros que los cifradores de flujo, a costa de ser más lentos y en algunas ocasiones requerir hardware especial dependiendo del tipo de cifrador. Sin embargo, es una opción que para comunicaciones donde el retardo no sea un factor determinante como en el caso anterior, ya que una comunicación por voz que se viese afectada por retardos en el proceso de cifrado podría hacer que el entendimiento entre los usuarios fuese imposible, puesto que en el caso de una comunicación que se dé lugar a través de internet, por ejemplo en una visita a una web, el impacto que puede tener un pequeño retardo en la petición de la página por parte del usuario no imposibilita para nada la comunicación y a cambio se obtiene una mayor seguridad.

Este ejemplo es una constante a la hora de securizar las comunicaciones, es decir, no sólo hay que ver cuánto de seguro es el sistema sino también el impacto que tendrá sobre la comunicación y si el coste asociado a esa securización es rentable, ya que invertir más dinero en un sistema de seguridad de lo que costase la propia información no tendría mucho sentido.

3.3.-Algoritmos de cifrado

Los algoritmos más conocidos que normalmente se suelen aplicar a los sistemas de cifrado por bloques son:

A.E.S (Advanced Encryption Standar): es un esquema de cifrado por bloques también conocido como Rijndael, que se basa en sustituciones y transposiciones. Es uno de los algoritmos más populares utilizados en criptografía simétrica que se transformó en estándar efectivo en el año 2002. Permite bloques y claves de tamaño variable, entre 128 y 256bits.

Es importante señalar, que antes de que se empezase a utilizar este sistema de cifrado, existía otro denominado D.E.S (Data Encryption Standar), que también se aplicaba en sistemas de cifrado por bloque y se basaba en operaciones de sustitución y permutación, aunque finalmente fue reemplazado por A.E.S ya que se detectaron importantes debilidades que permitían romper las claves en menos de 24 horas. Esto era debido a que el tamaño de la clave utilizado en D.E.S era muy corto, 56bits.

IDEA (International Data Encryption Algorithm): es un algoritmo que se basa en introducir confusión y difusión en el mensaje. La información se divide en bloques de 64bits y la clave tiene un tamaño fijo de 128bits. En un principio también fue planteado como un sustituto de D.E.S. Es un algoritmo muy robusto, en el que un ataque por fuerza bruta resulta impracticable con los medios informáticos de los que se disponen hoy en día, ya que se necesitarían probar 10^{38}claves.

En general, se puede destacar como ventajas de la criptografía simétrica su rapidez y su facilidad de implementación. Por contra, como desventaja, hay que señalar que los algoritmos utilizados no son tan seguros como los de criptografía asimétrica, y que además, en un entorno con n usuarios son necesarias n(n-1)/2 claves y un canal seguro para el intercambio de

todas estas claves, lo cual dificulta y complica la puesta en marcha de un entorno seguro basado en criptografía simétrica.

- ✓ ***Criptosistemas de clave pública o asimétricos:***

Los criptosistemas de clave pública surgen como la necesidad de resolver el inconveniente que se da en criptografía simétrica de intercambiar un número elevado de claves con la inseguridad que eso conlleva. Como solución intermedia se desarrolló el algoritmo de Diffie-Hellman, que es la base de la criptografía asimétrica, y permite el intercambio de una clave secreta de forma segura entre dos usuarios para después ser utilizada en soluciones de criptografía simétrica.

Su funcionamiento es el siguiente:

Dos interlocutores A y B, eligen un número primo p muy grande y un generador g. Ambos pueden hacerse públicos. Posteriormente realizan las siguientes acciones:

1. A elige un entero muy grande "x" y calcula $X = g^x mod\ p$ y se lo envía a B.
2. B elige otro número muy grande "y" y calcula $Y = g^y mod\ p$, y se lo envía a A.
3. A calcula $Y^x = g^{xy} mod\ p = K$.
4. B calcula $X^y = g^{xy} mod\ p = K$.

De este modo A y B pueden iniciar una comunicación protegida mediante criptografía simétrica, utilizando la clave K. Si algún intruso intercepta la comunicación durante el proceso de generación de la clave K, y capta el número Y y/o X además de conocer p y g, puede calcular $y = \log g\ Y\ mod\ p$ ó $x = \log g\ X\ mod\ p$. Sin embargo la realización de estas operaciones es casi inabordable ya que se necesitan computadores potentísimos.

La fortaleza de este algoritmo, y en general de la criptografía asimétrica, reside en la dificultad de factorizar números enteros muy grandes y en las propiedades de los números primos.
El paradigma de la criptografía de clave pública es que cada usuario cuente con una clave secreta intransferible y que no tiene la necesidad de compartir con nadie, y otra clave pública que puede ser conocida por todo aquel que desee intercambiar información con este usuario. Por supuesto, al igual que en el caso de la criptografía de clave secreta, los algoritmos de encriptación son de conocimiento público. Este tipo de criptosistema presenta como ventaja que se reducen el número de claves que hay que intercambiar en un escenario en el que intervienen varios usuarios y adicionalmente las claves secretas no tienen por qué viajar por la red, evitando así su interceptación.

La criptografía asimétrica es una solución de seguridad muy extendida dentro del comercio electrónico. Las plataformas de pago electrónico utilizan normalmente como base para proteger las transacciones de pago la criptografía asimétrica, empleándola en diferentes protocolos como https o SSL. En el caso de los pagos con tarjeta de crédito a través de internet, Visa desarrolló en colaboración con otras empresas los protocolos SET y su evolución 3D-Secure que también tienen su base en la criptografía asimétrica. Estos protocolos serán explicados con más detalle en capítulos posteriores.

El sistema más utilizado para cifrar en criptosistemas de clave pública se denomina RSA. Fue publicado por R. Rivest, A.Shamir y L.Adleman en el año 1977. Es un cifrador de modo bloque en el que el texto plano y el texto cifrado son enteros entre 0 y n-1, siendo n el tamaño de bloque y por lo tanto de la clave.

El funcionamiento del algoritmo es el siguiente:

- ***Generación de claves:***

  - ✓ *Clave pública:* está compuesta por dos números: n y e.

    Para formarla se eligen dos números primos p y q muy grandes (más de 100 dígitos decimales). Para más seguridad p y q deben de ser de la misma longitud. Una vez elegidos estos dos números se calcula n=p*q.

    Posteriormente se halla el indicador de Euler de los números primos p y q de la siguiente manera:

    $\varphi(n) = (p-1) * (q-1)$.

    Finalmente se calcula un número e, tal que sea primo relativo a $\varphi(n)$, y que cumpla m.c.d($\varphi(n)$,e)=1.

  - ✓ *Clave secreta:* está compuesta por dos números: n y d.

    Como la clave secreta y pública son para el mismo usuario, los números hallados en el paso anterior sirven para el cálculo de la clave secreta. Por tanto partimos de n y e para generar d.

    $d = e^{-1} mod\ \varphi(n)$.

- ***Cifrado del mensaje:***

  El algoritmo de cifrado se basa en la siguiente operación. Supongamos un mensaje en claro m. El criptograma resultante c de aplicar el cifrado RSA sería: $c = m^e mod\ n$. Si algún atacante intentase obtener el mensaje en claro m, tendría que realizar la siguiente operación $m = \log e^e\ c$, la cual es prácticamente inabordable.

El receptor del mensaje podrá descifrarlo como resultado de aplicar $m = c^d \ mod \ n$. En este caso se ha cifrado con clave pública y descifrado con clave privada, pero se puede aplicar el algoritmo a la inversa.

Como se puede deducir de las explicaciones anteriores, la criptografía asimétrica requiere mucho mayor potencial computacional y además el proceso de cifrado será más lento que en el caso de la criptografía simétrica. Pero como ventaja ofrece mucha mayor seguridad a la hora de proteger la información, y en el caso de pagos electrónicos la seguridad es una prioridad que prima sobre otros factores como pueden ser la rapidez o el excesivo consumo de recursos de un servidor a la hora de cifrar una comunicación, siempre y cuando estos no impidan llevar a cabo la comunicación con un tiempo y rendimientos razonables.

En el caso de la telefonía móvil, el desarrollo que están experimentando los terminales es en todos los aspectos asombroso, también a nivel computacional donde ya se integran procesadores casi de la misma potencia que en un PC, por lo que los requerimientos computacionales para la criptografía asimétrica no son a priori un impedimento para poder integrarlos en un terminal de telefonía móvil.

Otra de las ventajas de la criptografía asimétrica es que se puede combinar de varias maneras para ofrecer diferentes servicios de seguridad.

- *Para introducir autenticación del origen de los datos:*

Un supuesto usuario A, cifra un mensaje en claro con su clave secreta y posteriormente envía este mensaje a un segundo usuario B. El usuario B puede descifrar el mensaje conociendo la clave pública del usuario A.

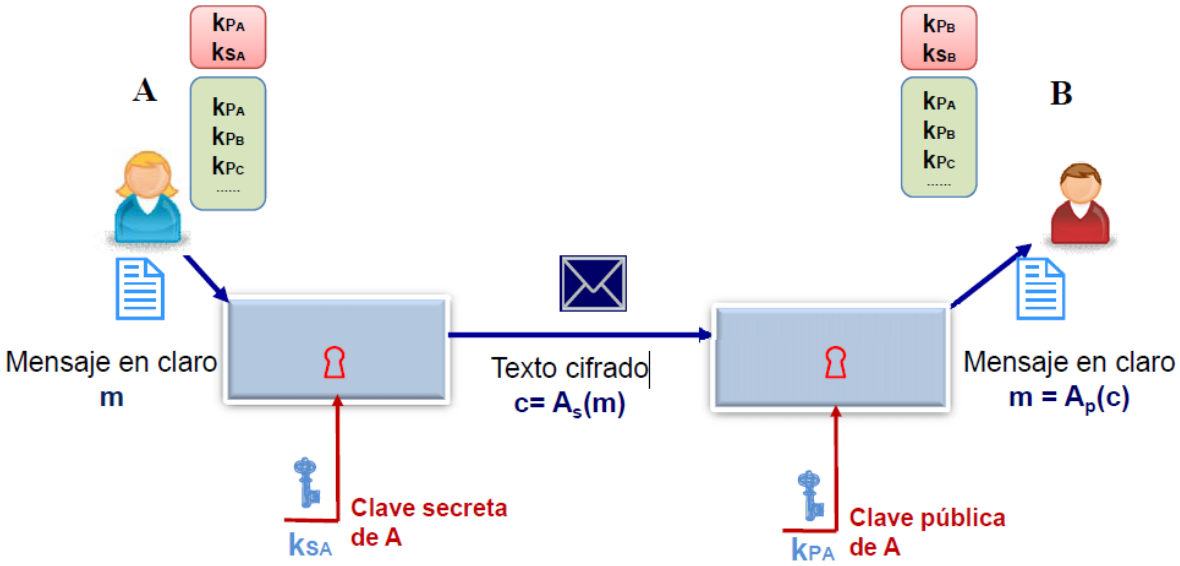

Figura 3.6

Este sería un buen ejemplo en el caso de que un banco u otra entidad como por ejemplo Visa quisiera autenticar a un usuario y le hiciese firmar los datos de la compra con su clave secreta. De esta manera la entidad se asegura de que el usuario que está intentando realizar la compra no es un usuario fraudulento.

- *Para introducir confidencialidad:*

Un usuario A cifra el mensaje con la clave pública del usuario B, con el que se quiere comunicar. El usuario B descifra el mensaje con su clave secreta. En este caso B y solo B puede descifrar el mensaje, ya que la clave secreta de B es intransferible.

Aunque son dos procedimientos diferentes de aplicar criptografía asimétrica, para obtener diferentes servicios de seguridad, estamos haciendo uso de la criptografía asimétrica en ambos casos.

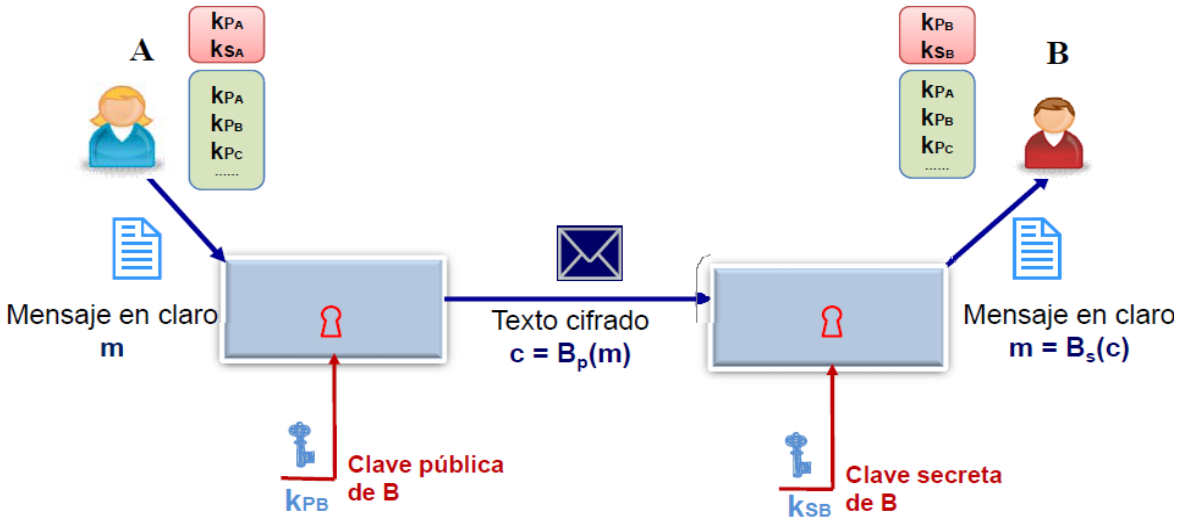

Figura 3.7

Otros ejemplos de los algoritmos utilizados en criptografía asimétrica son: El gamal, Merkle-Hellman, Rabin, Pohlig-Helman, etc. Estos algoritmos se basan en matemáticas mucho más complejas de exponenciación y factorización, por eso son más lentos que los de criptografía simétrica, pero por otro lado proporcionan más seguridad.

Actualmente se está investigando y desarrollando la criptografía de curvas elípticas, que es una variante de la criptografía asimétrica. Está basada en matemáticas de curvas elípticas y según los estudios realizados puede proporcionar mayor seguridad que RSA utilizando claves con menos bits. Todavía no se aplica en sistemas reales porque los estudios todavía no han concluido si este tipo de criptosistemas son fáciles de criptoanalizar.

Sin embargo, la criptografía de clave pública tiene fundamentalmente dos grandes problemas. Por un lado, que no es capaz de garantizar la integridad del mensaje por sí sola, ya que si se produce cualquier mínima modificación en el criptograma que es enviado hacia el destinatario no se puede asegurar cuando se descifre el mensaje y obtengamos el mensaje en claro que este haya sido alterado, y por otro, que para que se pueda usar de manera fiable hay que garantizar el origen de las claves públicas.

Para solucionar el primer problema se inventó la Firma Digital. La firma digital consiste en aplicar una función especial denomina Hash sobre el mensaje en claro que se quiera transmitir, dando como resultado un resumen del mensaje original, y firmar posteriormente este resumen con la clave secreta. Añadiendo esta pieza de información al mensaje que queremos transmitir, el receptor podrá probar la integridad y el origen de los datos recibidos.

Las funciones Hash realizan un resumen sobre el mensaje de entrada, produciendo una salida que siempre es menor y de tamaño fijo, independientemente del tamaño del mensaje de entrada. Son funciones que mapean un dato de un conjunto U, arbitrariamente grande, a un dato de un conjunto M cuyo rango de salida es finito, haciendo una proyección del conjunto U sobre el conjunto M.

Son funciones one-way, es decir, son fáciles de calcular en una dirección pero casi imposible de calcular en la dirección inversa. Además ante cualquier mínimo cambio en el mensaje de entrada la salida es totalmente diferente.

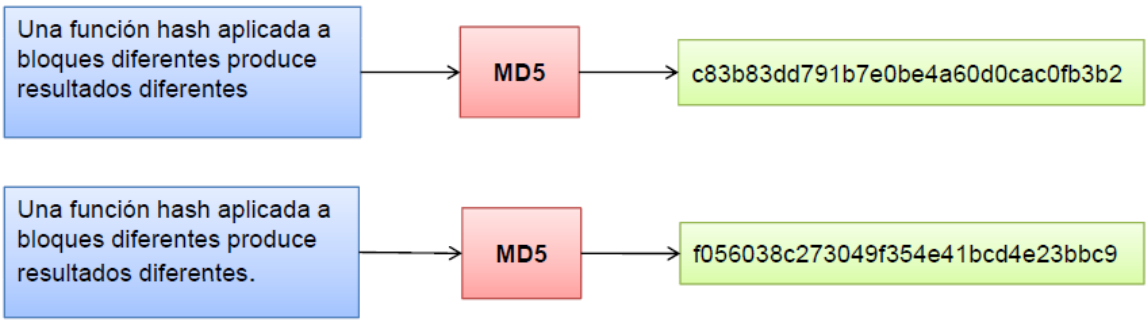

Figura 3.8

El algoritmo más usado para realizar resúmenes Hash es MD5. Genera un resumen de 128bits y es una evolución del antiguo algoritmo MD4. Aunque actualmente cada vez se tiende a usar más el algoritmo SHA, ya

que realiza resúmenes de 160bits que por lo tanto son más seguros frente a ataques de fuerza bruta.

Por tanto con ayuda de las funciones Hash se creó la Firma digital que permite añadir el servicio de integridad a una comunicación:

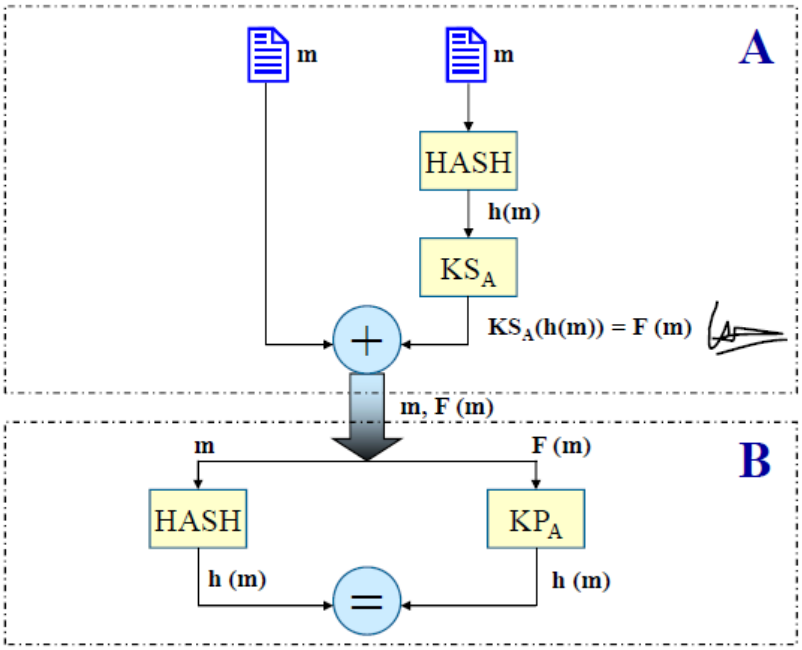

Figura 3.9

Como se puede observar en la figura anterior, el receptor B una vez recibe el mensaje y el hash encriptado con la clave secreta, es decir la firma digital, puede aplicar la función hash al mensaje en claro que recibe y desencriptar con la clave pública la firma digital, y ver que ambos resultados coinciden, certificando así la autenticidad de origen y la integridad del mensaje.

El servicio de integridad también es un servicio de seguridad muy importante dentro del comercio electrónico que es necesario implementar para evitar fraudes.

3.4.-Certificados digitales

El otro gran problema con el que cuenta la criptografía asimétrica es la necesidad de garantizar la autenticidad de las claves públicas.

La solución más extendida y utilizada para resolver este problema se denomina certificado digital. Se trata de un documento digital que está especificado en asn1 y estandarizado por el estándar X.509. Es expedido por una autoridad de certificación (CA), en la que los usuarios confían inicialmente, y que tiene como finalidad garantizar la autenticidad de la clave pública de un determinado usuario. La autoridad de certificación (CA), trata de emular la figura de un notario en el mundo real, de tal forma que pueda dar fe de la autenticidad de la clave pública de un usuario específico.

La CA es capaz de garantizar esta autenticidad, generando un documento en el que consta determinada información relativa al usuario al cual será expedido el certificado, y firmando digitalmente esta información. Como consecuencia de la firma con la clave secreta de la CA, todos los usuarios que inicialmente confíen en esa CA, pueden verificar la autenticidad de una determinada clave pública.

Como se ha dicho anteriormente, el certificado digital se rige por el estándar X.509, y está formado por muchos campos, pero los fundamentales son los siguientes:

- Versión del certificado. Actualmente existen tres versiones.
- Serial Number: es un número exclusivo, diferenciador de cada certificado.
- Nombre de la autoridad de certificación.
- Nombre distintivo de un usuario A, propietario de la clave pública.
- La clave pública del usuario A. Este es el campo más importante.
- Periodo de validez.
- Firma digital. (Firma de datos con la clave secreta de la CA).

Por supuesto, la autoridad de certificación como se ha indicado anteriormente tiene que ser de confianza para los usuarios. Muchas de las claves públicas de autoridades de certificación se instalan por defecto cuando se instala el S.O de un ordenador.

Las funciones principales de una CA son la de emisión y revocación de certificados. Para poder realizar estas funciones se ayudan de las PKI (public Key Infrastructure), que se trata de un conjunto de aplicaciones y servicios que permiten utilizar la criptografía de clave pública de una forma fácil y efectiva.

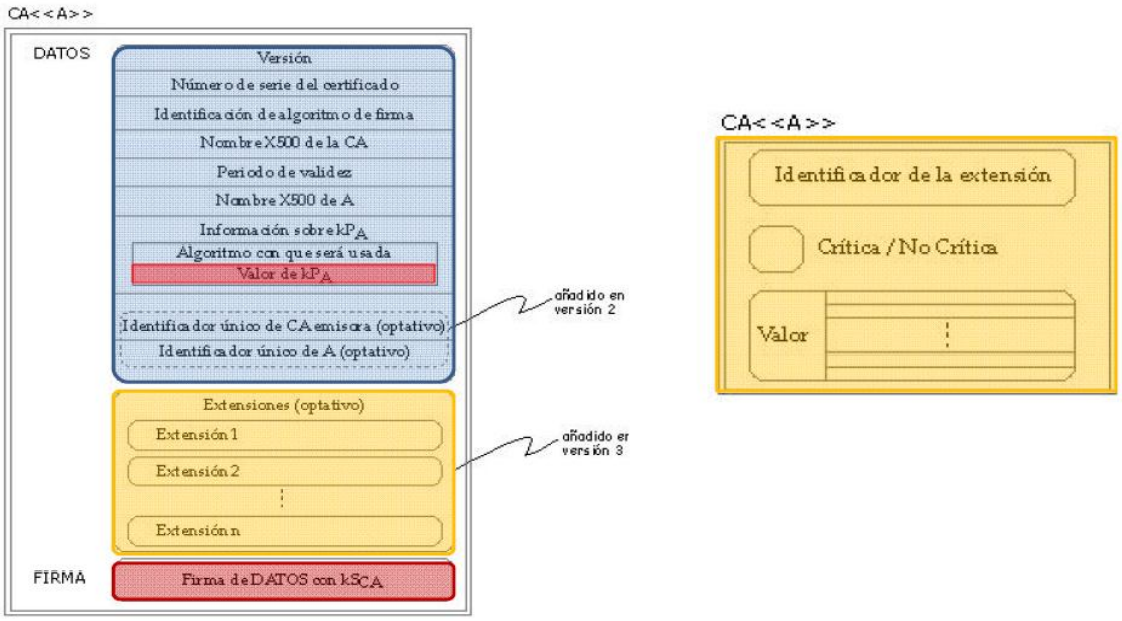

Figura 3.10

4.- SISTEMAS DE PAGO ELECTRÓNICO

Después de haber visto el capítulo anterior, donde se citan y explican conceptos básicos de seguridad necesarios para poder hacer uso del comercio electrónico, en este capítulo se explicará con más detalle alguno de los sistemas de pago electrónico más usados hoy en día, como es el caso del pago con tarjeta de crédito.

Dentro del comercio electrónico, el aspecto más importante y crítico que ha permitido desarrollar el e-commerce es el pago electrónico. Por decirlo de alguna manera, el pago electrónico es el núcleo alrededor del cual se desarrolla el comercio electrónico, y por otra parte no hay que perder de vista que el objetivo de este trabajo son los pagos con móvil. Pero antes de centrarnos en ellos y las diferentes soluciones que existen, vamos a ver algunos de los ejemplos que ya existen hoy en día y podemos usar a diario en nuestras vidas cotidianas.

4.1.-Tarjetas de crédito

El ejemplo más extendido y del que casi todo el mundo ha hecho uso es el caso del pago con tarjetas de crédito a través de internet. Las tarjetas de crédito son un recurso que se lleva utilizando desde hace mucho tiempo para realizar pagos electrónicos. La empresa más importante que emite este tipo de tarjetas se denomina Visa, y tiene su principal competidor en la empresa MasterCard.

Como dato histórico cabe resaltar que las primeras tarjetas de crédito fueron emitidas en el siglo pasado en el año 1914. Fueron emitidas por la empresa Western Union, y ofrecían una serie de facilidades a sus propietarios mediante acuerdos que tenían con otras empresas tales como hoteles, empresas de combustible, compañías de ferrocarril, etc. Por supuesto estas primeras tarjetas nada tenían que ver con las

sofisticadas tarjetas inteligentes con las que contamos hoy en día, ya que ni siquiera permitían el pago electrónico.

Hubo que esperar hasta principios de los años 80 para que apareciesen las primeras tarjetas de crédito electrónicas. Tecnológicamente son muy simples (en la actualidad todavía se usan), constan de una banda magnética cuyas partículas ferromagnéticas son polarizadas mediante una codificación determinada, y posteriormente esa información se puede leer mediante contacto físico, pasándolo a través de una cabeza lectora/escritora gracias al fenómeno de la inducción magnética. La estructura de las pistas está normalizada por la norma ISO/IEC7811.

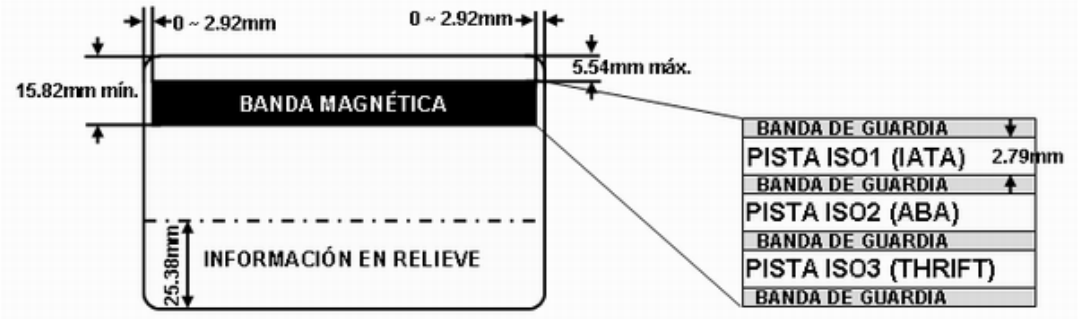

Figura 4.1

Las primeras tarjetas electrónicas se usaban para poder realizar extractos bancarios en cajeros automáticos, lo cual era muy cómodo para los usuarios ya que se evitaban restricciones horarias y en muchos casos geográficas, gracias a los acuerdos de interoperabilidad entre los diferentes bancos. Para la comunicación entre los cajeros automáticos y las entidades bancarias se utilizaban redes privadas gestionadas por los propios bancos. Eran redes ATM.

Pero tanto en España como en el resto del mundo, uno de los factores que sin duda impulsó el uso de las tarjetas de crédito electrónicas fue la integración de Puntos de Venta (P.O.S) por parte de los comercios, y que hoy en día todavía se siguen usando. El funcionamiento es muy simple, el consumidor adquiere el producto deseado en un local comercial que

disponga de un terminal de punto de venta (lo que conocemos como datáfonos), y mediante la utilización de la tarjeta de crédito/débito y un PIN para su autenticación, se realiza una transacción denominada "online" donde el coste del producto es cargado automáticamente en la cuenta bancaria del consumidor.

Aquí en España, en las primeras implementaciones de P.O.S, el comerciante se comunicaba con el banco mediante un terminal datáfono a través de la red telefónica básica y pasando por una red de datos (Red UNO) mediante la cual finalmente se comunicaban con el servidor bancario correspondiente.

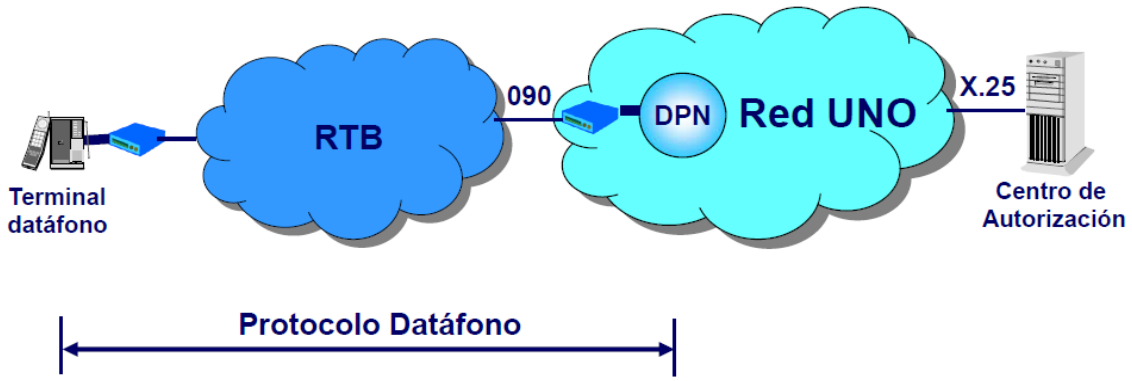

Figura 4.2

Actualmente la mayoría de los comercios utilizan el servicio de datáfono sobre ADSL, ya que permite operar con mayor velocidad, permite tener una misma línea para transacciones de voz y datos, y además todo ello se puede unificar en una tarifa plana. El esquema de comunicación cambia significativamente ya que en lugar de encaminar el tráfico de datos por la Red Telefónica Básica hasta llegar a la red UNO, ahora el tráfico es encaminado a través de la red IP previo paso por la red ATM de telefónica que brinda el servicio MegaviaADSL a los clientes.

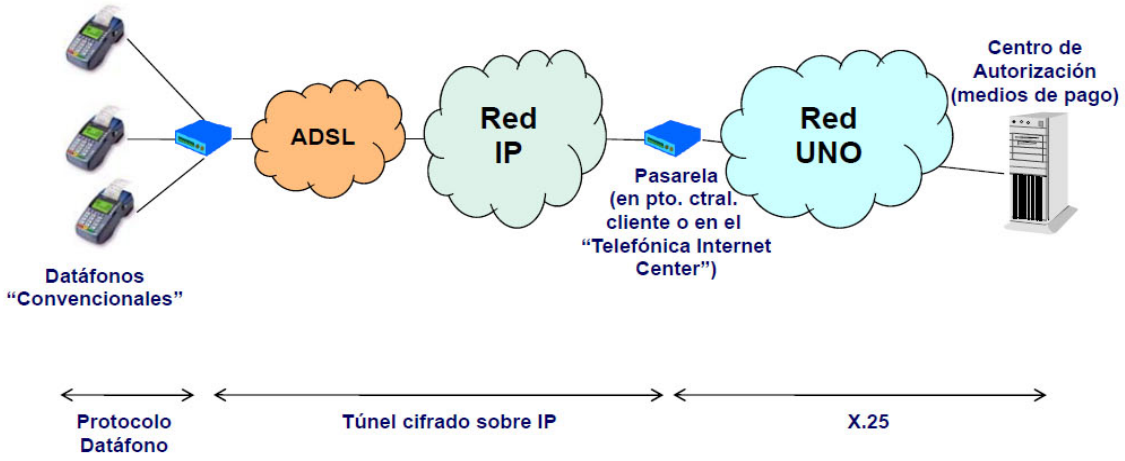

Figura 4.3

En esta última solución ya se puede ver la presencia de internet, lo cual significa el comienzo del comercio electrónico. Hasta ahora, las diferentes soluciones se desarrollaban sobre otro tipo de redes propietarias como la red UNO o la red de cajeros ATM, pero el comercio electrónico se empieza a considerar a partir de la aparición de internet como escenario principal en este tipo de transacciones.

Internet es una red pública que no está controlada y a la que todo el mundo puede tener acceso. Su flexibilidad y accesibilidad hacen que sea un buen escenario para desarrollar el comercio electrónico, pero por otra parte tiene la gran desventaja de que no es tan segura como las redes privadas ya que internet no está controlado por ninguna organización o entidad y cualquier usuario que esté conectado puede realizar ataques que afecten al resto de usuarios conectados. Teniendo en cuenta que en el comercio electrónico uno de los aspectos más importantes es el intercambio de datos bancarios para poder efectuar las compras, es necesario dotar a las comunicaciones que tienen lugar a través de internet de la seguridad necesaria para evitar cualquier tipo de ataque que pueda afectar tanto al acceso indebido como a la alteración de esa información. Además, un ataque malicioso también puede afectar a la seguridad de los sistemas que permiten este tipo de transacciones.

Debido a que actualmente los pagos con tarjetas de crédito se realizan a través de internet, vamos a analizar los diferentes protocolos de seguridad que se han desarrollado para proteger este tipo de comunicaciones. Aunque primero es necesario presentar el escenario y la arquitectura de comunicaciones que tiene lugar en los pagos a través de tarjetas de crédito.

En este escenario participan diferentes entidades que realizan varias tareas. Por un lado están los consumidores y los comerciantes, y por otro lado están los bancos y diversas asociaciones e instituciones que hacen de intermediarios y se encargan del manejo de las transacciones interbancarias. Realmente en este contexto, el titular de la tarjeta de crédito únicamente es consciente de la interacción con el comerciante y el banco, pero todo el desarrollo que tiene lugar más allá de estos dos participantes es totalmente transparente para los consumidores.

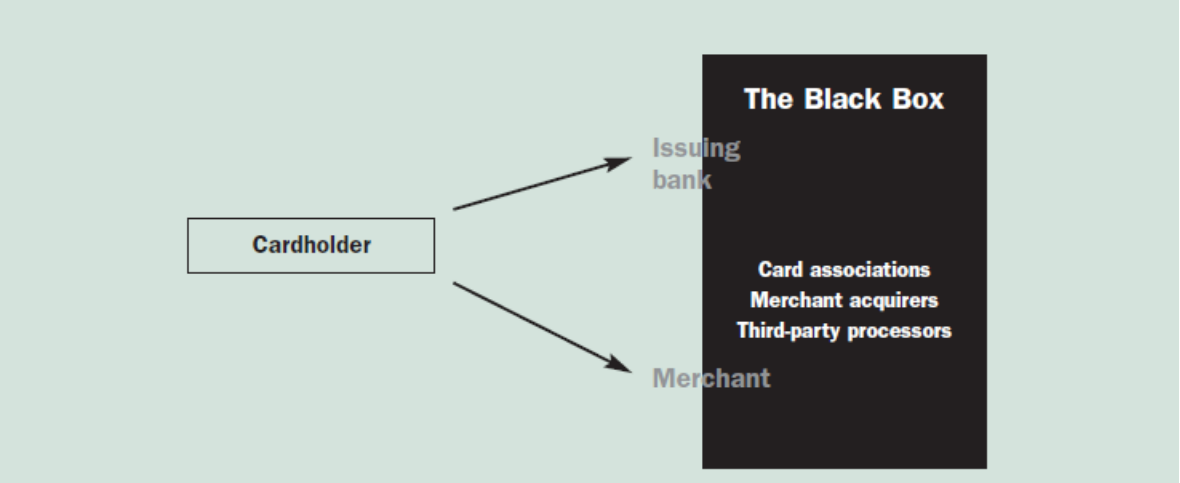

Figura 4.4

Vamos a ver el ejemplo de cómo es un pago realizado mediante una tarjeta de crédito a través de internet, concretamente con una tarjeta de la compañía Visa.

4.1.1- Transacción con una tarjeta de crédito:

Los pasos que tienen lugar para efectuar la compra son los siguientes:

1. El consumidor contacta con la web del comerciante para poder ver y elegir el producto deseado. Una vez ha elegido el producto, introduce los datos bancarios para realizar la compra.

2. Una vez el comerciante tiene los datos bancarios, envía una petición al Servidor de Visa.

3. El servidor de Visa a su vez envía una petición al Access Control Server (ACS) de Visa, y si la cuenta del consumidor está registrada dentro de Verified by Visa, el ACS retorna su dirección web de acceso hasta el comerciante.

4. El comerciante envía a través del consumidor, una petición de autenticación al ACS para que autentique al propio consumidor, utilizando la dirección que obtuvo en el paso anterior. El ACS muestra en el navegador del consumidor la interfaz de autenticación de verified by Visa, donde el comprador tiene que verificar y confirmar la información sobre la compra y validar la transacción introduciendo un PIN.

5. El ACS determina si la información introducida por el comprador es válida o no. Si la información no es correcta, el consumidor es notificado de que la transacción no se ha podido efectuar debido a que los datos no son correctos, y el comerciante puede elegir entre requerir otra forma de pago o declinar finalmente la transacción. Si los datos han sido validados correctamente, el ACS genera un mensaje de respuesta de autenticación válida y además genera un

valor criptográfico llamado valor de verificación de autenticación (CAVV), que enviará al comerciante para que sea usado más adelante durante la autorización de la transacción. Finalmente el ACS firma digitalmente el mensaje de repuesta de autorización con toda la información anterior. Todas las repuestas de transacciones de autorización son almacenadas en un servidor, tanto las aprobadas como las denegadas. El servidor se denomina Autentication History Server (AHS).

6. Si todo va bien el comerciante recibe la respuesta anterior firmada. Lo primero que hace es comprobar la veracidad de la firma, y una vez comprobada, si la firma es auténtica, genera una petición de autorización con el identificador de comercio electrónico (ECI) y el CAVV generado en pasos anteriores.

7. El proceso de autorización de adquisición recibe la información anterior y envía una petición de autorización a la red Visa Net.

8. Visa Net recibe la petición y se la transmite al emisor de autorización de compras por internet.

9. El emisor de autorización de compras por internet recibe la petición de autorización con toda la información recogida anteriormente. Este último realiza las comprobaciones necesarias con el banco del comprador, y si hay fondos suficientes autoriza la transacción, enviando un mensaje de autorización al comerciante. Si por cualquier razón, como por ejemplo falta de fondos, no se pudiese realizar la transacción, se devolvería un mensaje de petición denegada hacia el comerciante.

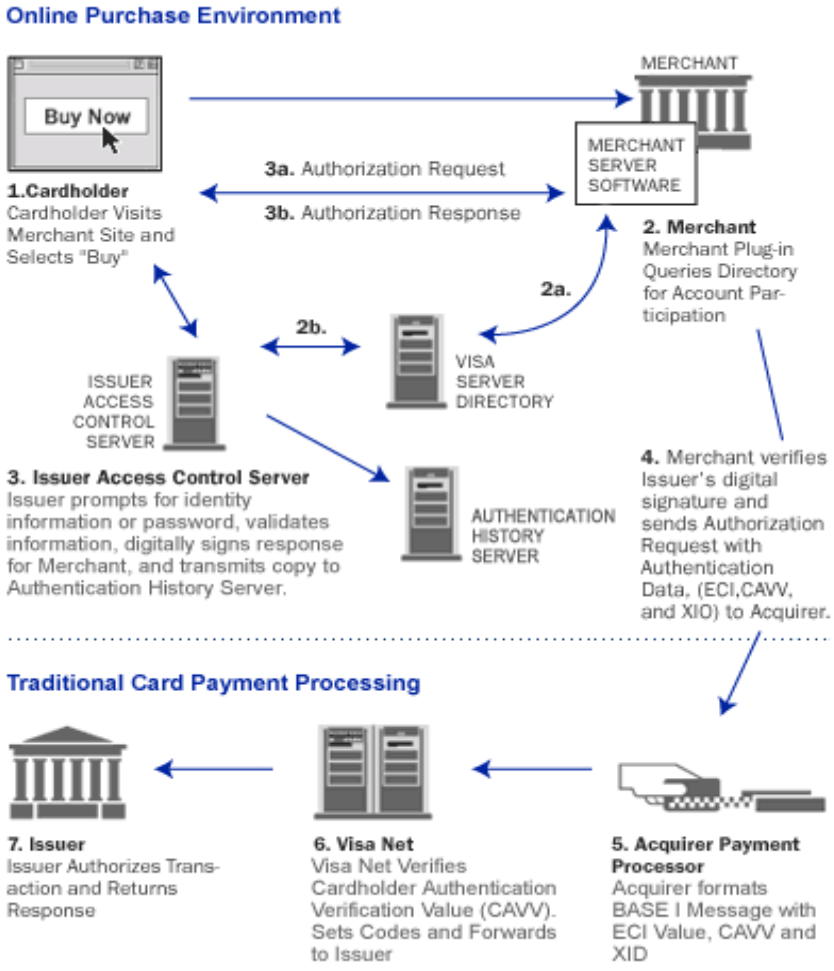

Figura 4.5

Una de las mayores vulnerabilidades que muestra el escenario anterior es el establecimiento de comunicaciones web entre los diferentes actores, ya que esta comunicación en la mayoría de las ocasiones es una comunicación que tiene lugar a través de internet. Adicionalmente, durante la transacción se llevan a cabo una serie de pasos donde es imprescindible garantizar la confidencialidad y sobre todo garantizar la autenticidad de todas las partes involucradas en el proceso.

Conscientes de este gran problema, hacia mediados de los años 90, Visa y MasterCard con la ayuda de otras compañías del sector IT, tales como IBM, Microsoft, RSA, VeriSign y otras, desarrollaron el protocolo SET

(Secure Electronic Transaction) que posteriormente fue estandarizado. Fue desarrollado para cubrir las vulnerabilidades que se han comentado en el párrafo anterior, añadiendo cómo principal novedad la verificación de identidades.

Pero antes de explicar el protocolo SET, y cómo este influye en una transacción de compra en el comercio electrónico, es necesario explicar el protocolo SSL, el cuál es la base del protocolo SET.

4.2.-Protocolo SSL

El protocolo SSL es un protocolo del nivel de transporte que protege la comunicación extremo a extremo. Puede proteger cualquier protocolo construido sobre socket: telnet, ftp, http…sin necesidad de hacer ninguna modificación sobre la aplicación, aunque fundamentalmente fue diseñado para dar protección a la comunicación entre un servidor y un cliente web. Los servicios de seguridad que proporciona son: integridad, confidencialidad y autenticación de origen y destino. El problema de SSL es que no está pensado para protocolos no orientados a la conexión, por lo que las aplicaciones que utilicen UDP como protocolo de transporte tendrán que valerse de IPsec si quieren securizarse.

SSL se vale de distintos subprotocolos, mostrando una arquitectura como la que sigue:

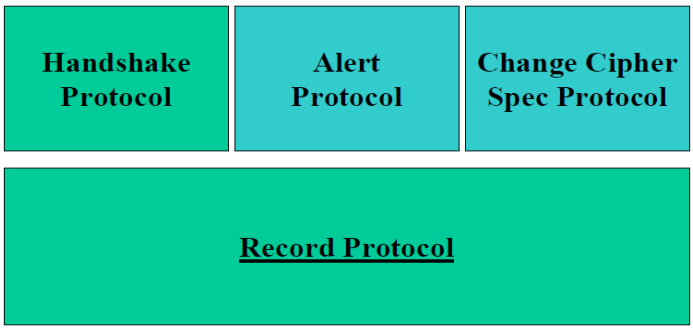

Figura 4.6

El handshake protocol, es la parte principal del protocolo SSL ya que se encarga de establecer y terminar las sesiones siguiendo los siguientes pasos:

1.- El cliente para establecer una sesión SSL envía un mensaje llamado ClientHello, que contiene lo siguiente: el nº de versión SSL, la fecha y hora actuales (sellos de tiempo), 28 bytes generados aleatoriamente, el identificador de sesión que el cliente quiere utilizar para esta sesión y las opciones criptográficas y medios de compresión soportados por el cliente.

2.- El servidor contesta con un mensaje ServerHello. Si el método de intercambio de clave no es anónimo, el servidor manda su propio certificado X.509v3 (ServerCertificate). Dependiendo del método de intercambio de clave utilizado (RSA, DH o Fortezza Kea), si el ServerCertificate no contiene la información necesaria para que el cliente pueda enviar el premaster key, se envía una clave para realizar el intercambio. Si se requiere autenticación de cliente se le solicita su certificado (CertificateRequest). Finalmente, el servidor envía ServerHelloDone.

3.- El cliente autentica al servidor. En caso de no poder autenticarlo avisa al usuario de que no puede establecer una conexión segura.

4.- El cliente crea el premaster secret, lo cifra con la clave pública del servidor y se lo envía.

5.- Si en el paso dos se solicitó autenticación del cliente, este envía algunos datos firmados junto con su certificado para dar muestra de estar en posesión de la clave secreta.

6.- Si se requirió autenticación del cliente se procede a validar su certificado. Si la autenticación falla, la sesión finaliza. En caso de continuar la sesión, el servidor obtiene el premaster secret descifrándolo con su clave privada. Tanto cliente como servidor, realizan una serie de cálculos para generar el master secret a partir del premaster secret.

7.- Cliente y servidor usan el master secret para generar las claves de sesión (sesión keys) que se emplearán para cifrar y descifrar y para chequear la integridad de la información.

8.- El cliente envía un mensaje al servidor indicándole que los mensajes serán enviados cifrados con las sesión keys. Para esto último se usa el protocolo ChangeCipherSpec, que sirve para cambiar entre un algoritmo de cifrado y otro habiendo una negociación previa entre cliente y servidor. Por último se envía un mensaje cifrado (Finished), indicando que el Handshake ha terminado.

9.- El servidor realiza las acciones del paso 8 hacia el cliente, finaliza el Handshake y la sesión SSL comienza.

Como se puede apreciar es un protocolo cuya función principal es autenticar a las dos partes que intervienen en la comunicación y encontrar una clave común para poder cifrar la comunicación, combinando el uso de la criptografía simétrica y asimétrica.

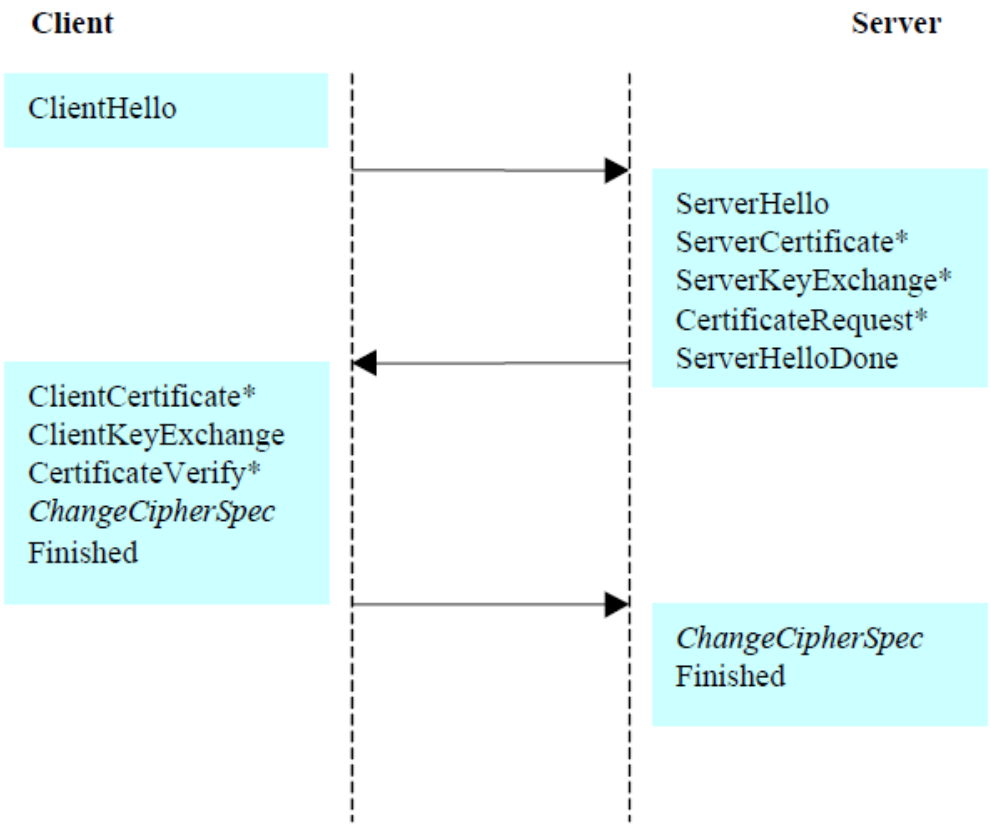

Figura 4.7

El protocolo llamado Alert Protocol es usado para indicar errores o condiciones de precaución a la otra entidad con la que se comunica. Define dos campos, uno de nivel de alerta, que pueden contener dos tipos, avisos indicando un problema no fatal, y fatales que terminan inmediatamente la sesión SSL. Y el otro campo es una descripción de alerta que describe el error más en detalle.

Finalmente, nos encontramos con la capa inferior de SSL, que se encarga de encapsular todos los mensajes proporcionando un formato común para los mensajes de alerta, de cambio de especificación de cifrado, de handshaking y de datos de usuario.

El protocolo TLS(Transport Layer Security), es la evolución de SSL. TLSv1 se basa y es compatible con SSLv3. Las mayores diferencias que presentan

son respecto a: Errores de alerta, cálculo diferencial del master secret, algoritmos de intercambio de claves soportados y el cálculo de MAC.

4.3.-Protocolo SET

La aparición del protocolo SSL fue vital para el desarrollo de posteriores protocolos como SET y 3D-Secure, ya que sentaba las bases para establecer una conexión web segura a raíz de la cual se podía trabajar para poder proyectar el comercio electrónico y los sistemas de pago.

Partiendo entonces de una comunicación web segura, ahora los esfuerzos se deben centrar en autenticar a todas las partes implicadas en el pago electrónico y gestionar todas las acciones derivadas de una acción comercial, para ello surge SET aportando los siguientes servicios de seguridad:

- *Autenticación*:

  Todas las partes implicadas en la transacción económica pueden autenticarse a través de los certificados digitales. Para ello el comerciante debe disponer de un certificado digital emitido por una CA, y el comprador debe de disponer de un certificado digital emitido por la entidad emisora de la tarjeta de crédito. Por supuesto, el banco también dispondrá de su certificado digital emitido por la correspondiente CA.

  De esta manera, el comerciante puede verificar la validez de la tarjeta del comprador, y el comprador puede validar la identidad del comerciante. Asimismo los bancos pueden verificar las entidades del titular y del comerciante.

- *Confidencialidad:*

  El aspecto más importante de la comunicación es proteger la información bancaria, para que, aunque alguien sea capaz de interceptarla no la pueda interpretar. Además también hay que garantizar la confidencialidad de los datos bancarios del comprador frente al comerciante, ya que solo la entidad bancaria debe acceder a estos. Para conseguir esto el comprador firma con la clave pública del banco sus datos bancarios de tal forma que solo el banco puede acceder a ellos. Cuando el comerciante recibe los datos bancarios del comprador firmados con la clave pública del banco, lo que hace es firmar esa información con la clave secreta, demostrando que la información ha pasado previamente por el comerciante. Este proceso también es conocido como firma ciega.

- *Integridad:*

  Gracias a diferentes algoritmos de hash utilizados en las propias firmas digitales, el protocolo SET es capaz de garantizar que la información intercambiada durante una transacción electrónica no ha sido alterada.

- *Gestión de pago:*

  Además de los servicios de seguridad, el protocolo SET se encarga de realizar las tareas asociadas a la actividad comercial desde el punto de vista de una entidad bancaria. Como por ejemplo: registro del titular y del comerciante, liquidaciones y autorizaciones de pago, anulaciones, etc.

Una transacción electrónica llevada a cabo a través del protocolo SET constaría de los siguientes pasos:

1. El comprador entra en la página web del comerciante y elige el producto que desea comprar. Rellena el formulario pertinente y cuando selecciona el botón de pagar el protocolo SET se activa.

2. El servidor del comerciante envía un certificado al navegador del cliente y un ID de transacción. También envía una descripción del pedido que despierta a la aplicación monedero del lado del cliente.

3. El cliente comprueba la descripción del pedido y el certificado del comerciante. En el caso de que esté de acuerdo con el pedido, el comprador envía su certificado al comerciante y la aplicación monedero genera un mensaje que irá cifrado con la clave secreta del comprador llevando la siguiente información: información del pedido, información del pago con los datos bancarios firmados con la clave pública del banco, una firma dual del hash de los datos del pedido y bancarios y un hash de la información de pago. Con este mecanismo se consigue que el comerciante pueda acceder a la información del pedido pero no a los datos bancarios.

4. El comerciante verifica el certificado del comprador. En caso de ser válido, el software SET del comerciante envía al banco su certificado y el del comprador, y firmado con su clave secreta la información bancaria del comprador, los detalles de pago, la firma dual que recibió del comprador y un hash de la información del pedido, para que el banco pueda contrastar la integridad de la información de pedido pero no pueda acceder a ella.

5. Finalmente, el banco verifica la información, obtiene la autorización del banco del cliente para poder realizar la transferencia de fondos y firma la autorización al comerciante para que pueda procesar el pedido.

Los mensajes de SET pueden ir sobre http en aplicaciones web, que suele ser la opción más habitual, pero también existe la posibilidad de que los mensajes SET sean transportados sobre correo electrónico, ya que no tienen la exigencia de transmitirse en tiempo real. Por otro lado, SET soporta transacciones con tarjetas de débito/crédito y también con tarjetas monedero, aunque estas últimas fueron añadidas más tarde debido a su naturaleza offline.

Para poder utilizar el protocolo SET es necesario tener instalada una aplicación en el ordenador llamada cartera digital (e-wallet). Esta aplicación fue especialmente diseñada para el uso protocolo SET. Simula la funcionalidad de una cartera tradicional y permite al usuario tener guardados los números de las tarjetas de crédito además de almacenar los resguardos de las diferentes compras realizadas. Toda esta información junto con el certificado del usuario y del banco se encuentran protegidos con un sistema complejo de encriptación simétrico.

Entre las debilidades de SET se puede destacar la lentitud del proceso, al tener que realizarse diferentes verificaciones de identidad e integridad por parte de diversas entidades a lo largo de una transacción, y la infraestructura de CAs requerida para emitir certificados a compradores y vendedores así como el coste de su implementación.

También dificulta su utilización el tener que disponer de un software adicional, tanto para el comprador como para el comerciante, y que los ISP soporten el protocolo.

Como evolución natural de SET surgió el protocolo 3D-Secure, desarrollado por Visa y que añade como principal novedad respecto a SET que es capaz de verificar que el comprador está autorizado a usar la tarjeta que le proporciona al vendedor, de ahí su nombre comercial Verified By Visa, el cual ya vimos aplicado en el ejemplo de la página 39 y 40.

Al igual que SET, 3D-Secure se apoya en SSL para garantizar la seguridad de los mensajes intercambiados. A la hora de realizar una compra tiene un funcionamiento muy simple. 3D-Secure solicita al usuario una clave que éste ha tramitado previamente con su banco emisor. Si la clave es correcta y la tarjeta dispone de crédito, el sistema autoriza la compra. Esto se puede ver en el paso 4 del ejemplo de pago mediante una tarjeta de crédito Visa en la página 39. Los pasos detallados que se dan durante una transacción llevada a cabo con 3D-Secure son los mismos que los detallados en esa misma página, a través del ejemplo citado.

Como gran ventaja, este protocolo evita el uso fraudulento de tarjetas de crédito a través de internet, el cual puede generar muchas pérdidas tanto para los comerciantes como para los usuarios cuyas tarjetas son utilizadas de manera ilegítima.

Además 3D-Secure es muy fácil de adoptar tanto para consumidores como para vendedores. Los vendedores solo tienen que añadir un plug-in a sus servidores de comercio electrónico y los compradores, por su parte, no tienen necesidad de instalar ningún software adicional ni adquirir ningún dispositivo para poder disfrutar de las ventajas de 3D-Secure.

Como contrapartida, hay que señalar que 3D-Secure tampoco es infalible, ya que algunos usuarios han sido víctimas de ataques de phising al no saber diferenciar entre una ventana emergente de Visa By Verified y una fraudulenta. Aunque realmente, para contrarrestar este tipo de ataques

también existe un protocolo denominado https que igualmente se basa en SSL.

La diferencia entre http y https se puede apreciar en el navegador cuando introducimos la dirección URL de la página a la que queremos acceder. En el caso de estar utilizando https, las URLs siempre empiezan por https://...

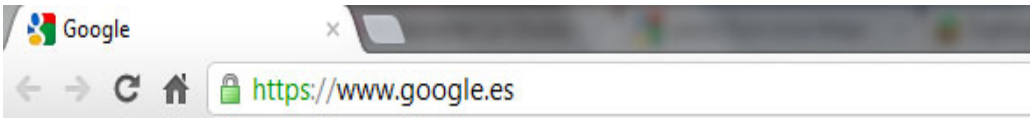

Figura 4.8

Al fundamentarse en SSL, cuando queremos establecer una conexión https, el servidor web al cual nos conectamos debe disponer de un certificado de clave público X.509v3, y ese certificado tiene que estar firmado por una CA en la cual confía nuestro navegador. Cuando instalamos el navegador en nuestro PC, ya vienen por defecto una serie de CA raíz y CA intermedios instalados.

Si se da el caso de que el Certificado del servidor web está firmado por una CA en la cual no confía nuestro servidor, en el navegador nos aparecería un mensaje de aviso como el siguiente:

Figura 4.9

Actualmente las especificaciones de 3D-Secure también son aceptadas por MasterCard y JCB.

4.4.-Otros ejemplos de pagos electrónicos

A parte de los sistemas de pago con tarjetas de crédito, que son los más extendidos, han aparecido y están apareciendo cada vez más soluciones diferentes para realizar pagos a través de internet, como es el caso de las e-wallet.

Estas aplicaciones no tienen ninguna vinculación con ninguna entidad bancaria, se pueden adquirir desde internet gratuitamente para el consumidor, no así para el comerciante, y simplemente se instalan en el PC personal del comprador. Una vez instalado se introducen los datos personales del usuario incluyendo sus datos bancarios independientemente del banco al que pertenezca el usuario. La gran ventaja de estos sistemas es que cada vez que se entre en una página web distinta para realizar una compra, no se tendrán que introducir los datos bancarios de nuevo, porque bastará con haberlos introducido una sola vez al principio, haciendo así las compras más rápidas y eficientes.

Los datos de los usuarios son debidamente encriptados y guardados online, en los servidores particulares de la compañía que ofrece el servicio, para que los datos estén disponibles en red y se pueda acceder a ellos cuando se necesite, sin tener ninguna vinculación a un dispositivo en concreto.

Este tipo de aplicaciones se pueden utilizar o bien como monedero electrónico, donde se registraría un determinado e-cash en la aplicación para poder realizar las compras, o se le puede dar el uso de una tarjeta de crédito normal donde la transacción y el cobro se realizarán online. Algunos ejemplos de estas aplicaciones que están cobrando éxito son amazon payments y google checkout.

Figura 4.10

Otro de las soluciones bastante extendida para poder pagar por internet es el caso de Paypal. Se trata de una empresa que actúa como una tercera parte de confianza entre en comprador y el vendedor, suplantando el papel de una entidad financiera.

Paypal es una empresa estadounidense propiedad de Ebay y referente en el comercio electrónico. Permite realizar pagos electrónicos a través de internet actuando como un intermediario entre los compradores y los vendedores.

Para poder abrir una cuenta en paypal y poder realizar los pagos a través de esta plataforma, los únicos datos necesarios son un correo electrónico que identifique al usuario y una contraseña.

A esta cuenta habrá que asociar una tarjeta de crédito/débito y/o una cuenta corriente. Una vez se registre toda esta información en la cuenta Paypal, no será necesario volver a introducir ningún dato bancario por parte del comprador, simplemente tendrá que facilitar su correo electrónico y la contraseña para acceder a su cuenta Paypal, que a su vez estará vinculada a una tarjeta de crédito, de débito o a una cuenta bancaria corriente para realizar los pagos.

Adicionalmente se suele crear una cuenta de fondos Paypal donde se puede depositar dinero o extraerlo hacia la cuenta bancaria, o también hacer transferencias a otro usuario de Paypal con simplemente disponer de su dirección de correo electrónico.

Para realizar un pago con Paypal, el comerciante nos tiene que facilitar esa opción. En el caso de que si nos facilite esa opción, tendrá un icono en su

página web que nos conectará con el servidor de Paypal donde nos tendremos que autenticar, y a partir de ahí Paypal se encarga de realizar el pago facilitando el envío de dinero desde varias fuentes hacia diferentes destinatarios, con la ventaja de no tener que compartir la información financiera con el comerciante.

Por supuesto para garantizar la seguridad, todas las conexiones que tienen lugar con el servidor de Paypal van sobre el protocolo SSL.

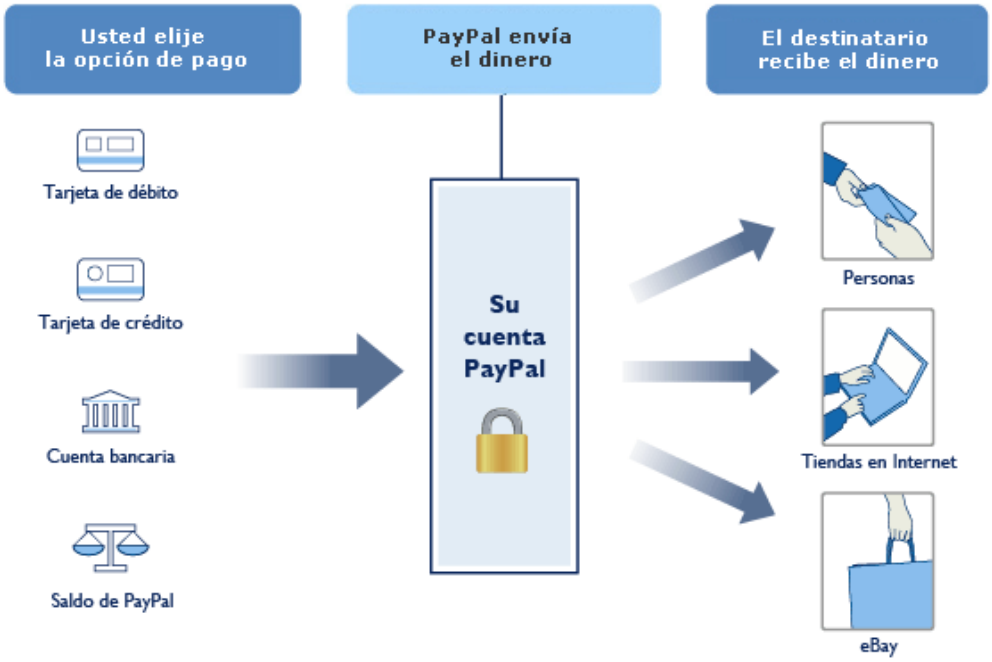

Figura 4.11

Todas las notificaciones de pago o ingreso que tienen lugar a través de la plataforma Paypal se realizan mediante el correo electrónico.

Como desventajas de este sistema se puede señalar que debido a que los pagos se realizan por medio de correos electrónicos, es un sistema muy susceptible de ataques de phising, donde los enlaces de correo electrónico son fácilmente redirigibles hacia portales fraudulentos. Por otra parte, como todas las notificaciones se realizan via mail, se corre el riesgo de que

alguna notificación importante sea capturada como Spam por los filtros antiSpam.

Además, este sistema puede ser muy apropiado para acometer actividades ilegales de blanqueo de dinero, ya que Paypal al no ser un banco propiamente no está sujeto a las regulaciones bancarias.

5.- EL TERMINAL MÓVIL

Los terminales de telefonía móvil han experimentado una enorme evolución tecnológica en los últimos años, lo cual ha permitido que además del uso tradicional que siempre se le ha dado se pueda emplear para otros usos. Realmente el factor que ha favorecido su evolución tecnológica es que el móvil se ha convertido en un dispositivo imprescindible en nuestro día a día. Sólo en España, el mercado de teléfonos móviles cuenta con más de cuarenta millones de usuarios y esto ha supuesto que todas las empresas implicadas en el sector de la comunicación móvil se hayan movilizado para investigar y desarrollar nuevas utilidades que sean del agrado de los usuarios para poder seguir generando beneficios y abriendo nuevas áreas de negocio.

Para poder desarrollar nuevas utilidades y ofrecer nuevos servicios a los usuarios, los terminales móviles han ido sufriendo una evolución tecnológica progresiva donde cada vez se van integrando más funcionalidades, así por ejemplo, comenzaron integrando cámaras fotográficas en el móvil, siguieron desarrollando pantallas cada vez más grandes hasta llegar a interfaces multitáctiles, al mismo tiempo que aumentaban las capacidades de procesamiento integrando procesadores muy potentes intentando simular la capacidad de un PC, lo que a su vez permitió el avance en sistemas operativos para móviles, que cada vez son más versátiles y permiten al usuario disponer de infinidad de aplicaciones que pueden ejecutar para obtener diferentes servicios. Es pues en este punto dónde nos encontramos, donde los terminales móviles ya no son únicamente terminales inalámbricos de telefonía que sirven para llamar y enviar sms, sino que disponemos de smartphones que nos ofrecen una gran cantidad de funcionalidades y abren la puerta a nuevos servicios para los usuarios.

Uno de esos nuevos servicios que cada vez está teniendo más importancia es el pago por móvil, el cual es un servicio realmente atractivo por su comodidad y seguridad y porque para la empresa que ofrezca este servicio le supone un extraordinario valor añadido.

Pero antes de meternos de lleno en lo que son los sistemas de pago con móvil, se va a explicar brevemente algunas partes internas de un teléfono móvil que serán interesantes de cara a la realización de los pagos.

Dentro del mundo de las comunicaciones móviles, el teléfono móvil es denominado "estación móvil" normalmente mediante las siglas MS. En lo que se refiere a la estación móvil, a parte de todos los avances que se han comentado anteriormente que han permitido evolucionar a las estaciones móviles hasta lo que hoy conocemos como smartphones, tienen todas un elemento en común que es fundamental. El módulo SIM.

5.1.-La SIM

Internamente todas las estaciones móviles cuentan con el módulo SIM (Suscriber Identity Module). Se trata de una pequeña tarjeta inteligente que contiene toda la información relativa al abonado y puede ser utilizado en cualquier otro terminal compatible. Entre la información más importante que guarda la SIM se encuentra la siguiente:

- Número de serie
- Identificación internacional del abonado móvil (IMSI)
- Identificación temporal del abonado móvil (TMSI)
- PIN (Clave corta de desbloqueo)
- PUK (Clave larga de desbloqueo)
- Clave del algoritmo de autentificación (Ki)

- Algoritmo de autentificación (A3)
- Algoritmo de generación de claves de cifrado (A8)
- Algoritmo de cifrado (A5)
- Clave del algoritmo de cifrado (Kc)

Como se puede ver, toda la información que se ha resaltado sobre el módulo SIM es información de seguridad que solo puede estar en posesión del abonado para evitar cualquier tipo de fraude posible. En general se trata de claves necesarias para poder autenticar al usuario en la red de comunicaciones móviles y claves para poder cifrar la comunicación.

Auntenticación:

Antes de que el usuario puede acceder a la red, tiene que demostrar que es un abonado autorizado para poder utilizar la red. Para ello el abonado en primer lugar manda a la red una petición de uso a la red y esta le contesta mandándole un número aleatorio. Con ese número y la aplicación del algoritmo A3 y la clave Ki se obtiene otro número resultante que es el que el terminal móvil envía a la red. Esta previamente ha realizado el mismo cálculo que el terminal móvil y al ver que el número es correcto autoriza al abonado a utilizar la red.

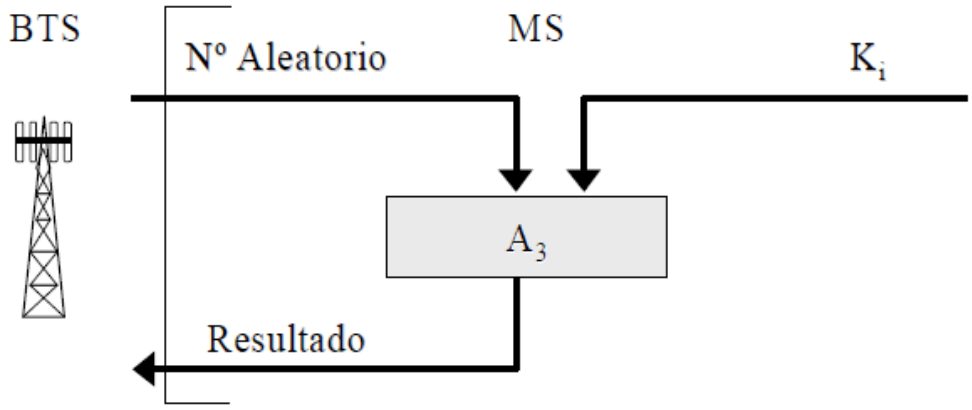

Figura 5.1

Encriptación:

Después de que el abonado ya se haya autenticado y esté en disposición de utilizar la red, el siguiente paso es establecer la comunicación, pero esta ha de ir encriptada. Hay que señalar que las comunicaciones digitales móviles desde la segunda generación (GSM) van siempre encriptadas. No solo se encriptan los datos de usuario sino que también se encripta la señalización. Esto es importate ya que los sms que son utilizados como forma de pago en algunas soluciones van sobre canales de señalización. Nuevamente para realizar este paso la red envía un número aleatorio al terminal móvil que haciendo uso del algoritmo A8 y la clave Ki calcula una nueva clave que junto con el algoritmo A5 se aplica a toda la información que sale del terminal móvil. Como se trata de criptografía simétrica en el lado de la estación base se aplica el mismo proceso para desencriptar.

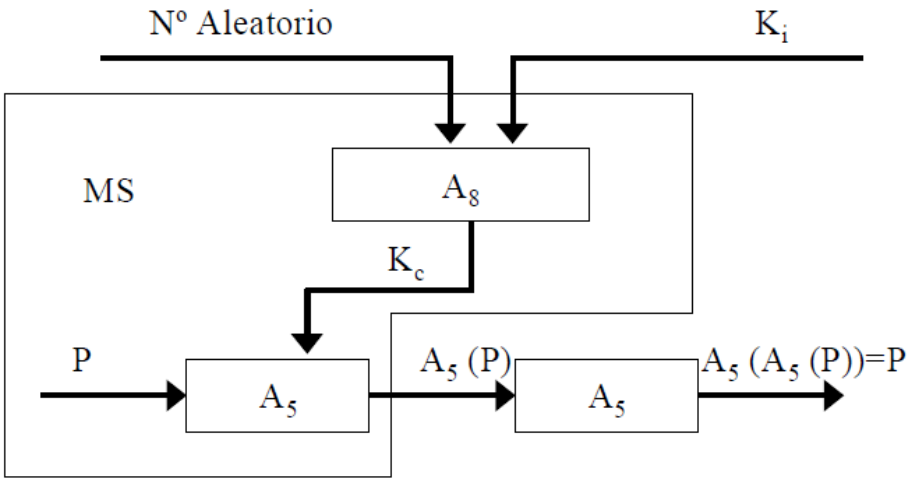

Figura 5.2

La comunicación cifrada solo tiene lugar entre el móvil y la estación base, que es el tramo más sensible a posibles intrusiones.

Es importante resaltar estos procedimientos de autenticación y encriptación que tienen lugar gracias al módulo SIM, ya que como se verá

más adelante, las soluciones de pago con móvil que utilizan el servicio sms para realizar los pagos o una simple llamada telefónica, queda demostrado que van encriptadas y por tanto protegidas frente a posibles ataques de interceptación de datos personales y bancarios. Todo ello se lleva a cabo haciendo uso de la criptografía simétrica.

Por tanto el módulo SIM, es un elemento fundamental del terminal móvil para poder establecer una comunicación. Además de la información de seguridad que se ha señalado anteriormente, también guarda información adicional:

- Estado de la tarjeta
- Código de servicio
- Datos personalización
- Información de localización temporal (LAI)
- Estado de función de roaming
- Estado de validación
- Estado función de activación/desactivación PIN
- Estado del PIN
- PIN (Personal Identification Number)
- Contador errores PIN
- PUK (PIN Unblocking Key)
- Lista de redes prohibidas
- Mensajes cortos recibidos
- Nº directorio autorizados
- Estado llamadas salientes

Realmente la SIM es una tarjeta inteligente que además de permitir guardar los datos encriptados bajo una clave permite hacer pequeñas operaciones y realizar cierto procesamiento de datos. A alto nivel la SIM tendría una estructura como la siguiente:

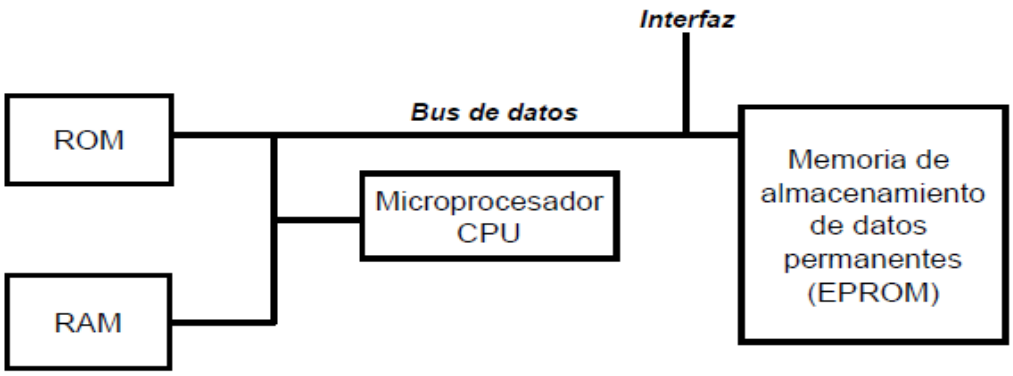

Figura 5.3

Estas características de la SIM son muy interesantes de cara al pago con móvil, como se podrá ver más adelante, ya que en el caso de que se quieran guardar los datos bancarios de un usuario en el móvil, la tarjeta SIM se podría aprovechar para ello, sin necesidad de añadir ninguna pieza de hardware adicional al móvil.

Por último en este capítulo, destacar que toda esta descripción que se ha realizado es para GSM (Global Systems for Mobile Communications), que es la segunda generación de las redes de comunicaciones móviles. Como evoluciones posteriores vinieron GPRS (General Packet Radio Service) que es considerada 2,5G y permitió mejores prestaciones en el acceso móvil a servicios de datos e internet, lo cual también es un factor muy interesante de cara a los pagos por móvil, porque disponemos de internet como plataforma para poder realizar los pagos electrónicos. Más tarde vino la 3G, conocida como UMTS (Universal Mobile Telephone System) para mejorar las velocidades de acceso a internet permitiendo el acceso a una densidad mayor de usuarios. En UMTS, el módulo SIM es conocido como USIM, pero contiene la misma información que en el caso de GSM, y los procedimientos de autenticación y cifrado son similares, aunque más potentes a los empleados en GSM, al igual que en el resto de generaciones.

6.-EL PAGO CON MÓVIL

El pago con móvil, también conocido como m-commerce o m-payment, consiste fundamentalmente en realizar pagos o transacciones entre particulares a través del terminal móvil. Las ventajas que principalmente ofrece poder realizar los pagos mediante el teléfono móvil son que permite realizar las transacciones de manera rápida, cómoda y segura, y que se puede hacer en cualquier momento y desde cualquier lugar.

Existe un amplio abanico de soluciones de pago con móvil, lo cual supone una gran ventaja ya que el pago con móvil se puede llevar a cabo con cualquier terminal móvil de telefonía y sobre cualquiera de las redes de telefonía móvil que existen operando en nuestro país, GSM, UMTS…
Otra de las flexibilidades que muestran los sistemas de pago con móvil, es que puede estar asociado o no a una entidad financiera. Es decir, como veremos más adelante, hay sistemas de pago en los que es necesario tener asociado una o más tarjetas de crédito o débito, pero también existe la posibilidad de que el sistema de pago no esté asociado a ninguna tarjeta y los cobros sean cargados directamente en la factura del proveedor de servicios. Esta también es una de las peculiaridades que se analizarán, dado que hay proveedores de servicio, sobre todo en países en vías de desarrollo, que juegan el papel de entidad financiera.

La seguridad es otro de los aspectos que favorece el pago mediante móvil, ya que tanto las redes GSM como las UMTS reúnen como hemos podido ver, medidas de seguridad adecuadas para poder realizar el pago mediante el móvil. Además, para poder malversar una tarjeta de crédito, basta con tener su número y fecha de caducidad sin necesidad de tener su posesión física, sin embargo para malversar un terminal móvil como sistema de pago es necesario estar en posesión física del terminal, conocer el código de seguridad que da acceso a la SIM, y conocer el código

que permite realizar las transacciones de compra, que como se verá se denomina NIP.

Otra de las cosas que es posible realizar gracias a los pagos con móvil, es la transferencia de dinero entre usuarios sin necesidad de acudir al banco, y en algunos casos sin necesidad de conocer los datos bancarios de la otra persona, ya que el dinero transferido al otro abonado será ingresado en la cuenta bancaria asociada al teléfono (SIM).

Por último cabe destacar como ventaja, que las comisiones que se aplican al pago con móvil son muy reducidas. Por poner dos ejemplos de plataformas de pago móvil que operan en España, Mobipay aplica una comisión de 0,08€ por operación realizada y Paybox aplica una cuota anual de unos 12€, y en lo que concierne al comerciante, las cuotas también son menores ya que a las entidades bancarias se les aplica una comisión mucho menor que en el caso del pago con tarjeta, y como ventaja los comerciantes tienen menor riesgo que en el pago con tarjeta.

A pesar de las principales ventajas que muestra el pago con móvil, precio, facilidad de uso, fiabilidad y seguridad, hay que reconocer que excepto en los países asiáticos, aún es método de pago cuya aceptación está todavía por madurar, de igual manera que ocurrió en su día con las tarjetas de crédito que eran vistas como un medio de pago reservado para personas con alto poder adquisitivo. Por tanto, en este sentido, digamos que el pago por móvil está atravesando la evolución natural que sufre cualquier tecnología emergente.

El otro factor que está influyendo enormemente en la evolución del pago por móvil es la falta de una solución abierta. Actualmente, lo que están haciendo los comercios es asociarse con una plataforma de pago por móvil determinada, de tal forma que si un usuario no está dado de alta en esa plataforma de pago por móvil no podrá realizar el pago con su terminal móvil, lo cual supone un gran inconveniente. Pero frente a esto, el pago por móvil también ofrece la ventaja de que se puede estar dado de alta en varias plataformas de pago por móvil a la vez utilizando el mismo terminal,

no como pasaba con las tarjetas de crédito, que había que poseer una por cada plataforma de pago diferente.

Pero sin embargo, a pesar de su lenta aceptación, el pago con móvil se muestra como un medio idóneo para poder realizar pagos en aquellas circunstancias donde las tarjetas de crédito no son aceptadas o cuando disponer del importe exacto que se necesita es muy complicado, como puede ser el caso de entregas a domicilio, taxis, máquinas expendedoras, etc.

7.- PLATAFORMAS DE PAGO CON MÓVIL

Actualmente existen diferentes plataformas de pago con móvil que se podrían clasificar teniendo en cuenta varios factores. Por ejemplo, podríamos hacer una clasificación ateniéndonos al tipo de tecnología usada, o en base a si el sistema de pago está ligado a una cuenta bancaria, o si los datos bancarios están guardados y disponibles siempre en el terminal móvil, o si se trata de plataformas de pago móvil u online, etc.

En este trabajo se va a realizar una clasificación según la tecnología empleada en el sistema de pago ya que es el factor y la característica más influyente en el funcionamiento del mismo. De todas formas, en cada uno de los sistemas que se presenten se detallarán todas las características que lo caractericen.

7.1.-Plataformas de pago con SMS

Cuando despegó la telefonía móvil, el sms fue uno de los servicios que se añadió y partía como un servicio totalmente secundario. Es un servicio de mensajes cortos (140-160 caracteres), que permite el envío de mensajes entre teléfonos móviles y fijos aprovechando los canales de señalización. Sin embargo, con el paso del tiempo se comprobó cómo los usuarios comenzaron a darle un uso mucho mayor del que en un principio se esperaba, convirtiéndolo en un servicio casi esencial. En un principio fue diseñado como parte del estándar de telefonía móvil digital GSM, pero hoy en día está disponible en una amplia variedad de redes.

Pues bien, debido a que el SMS es uno de los servicios ampliamente adoptado por los usuarios de telefonía móvil, se aprovechó para utilizarlo como solución en los sistemas de pago con móvil.

El servicio de sms es ampliamente soportado tanto por terminales de telefonía muy simples como por los terminales más avanzados (smartphones), y por otra parte, es un servicio que se puede utilizar fácilmente ya que no presenta complejidad alguna. Como desventaja se puede señalar que hoy en día el coste que conlleva el envío de un sms puede ser relativamente mayor al coste que implican otros canales de comunicación mediante el móvil, ya que el coste de un sms ronda los 0,15€, mientras que una tarifa plana de datos puede costarnos una media de 20€/mes y podemos tener acceso a internet las 24h del día. Sin embargo, también hay que tener en cuenta que en países en vías de desarrollo puede ser un canal de comunicación muy útil debido a que no necesita de ninguna sofisticación en el terminal móvil y puede ser de fácil acceso para cualquier usuario.

En general, un sistema de pago con móvil basado en el servicio de sms, consta de los siguientes elementos*:*

7.1.1.-Arquitectura:

El usuario con terminal móvil. El usuario tiene que darse de alta en una plataforma de pago con móvil y asociar una tarjeta de crédito o débito al número (SIM) de su terminal móvil, de tal manera que cuando realice una compra el importe de la misma sea cargado a dicha tarjeta. Dado que los sistemas de pago móvil basados en sms no son online, el dinero no tiene porqué ser deducido de la cuenta en el mismo momento que se realice la compra.

Una plataforma de pago que se encargue de gestionar la comunicación entre el comprador y las entidades financieras. Esta parte es fundamental, ya que sin ella no se podría realizar el pago con móvil y es común en los primeros sistemas de pago con móvil que se desarrollaron.

En este caso, la plataforma se encargará de recibir las peticiones de pago procedentes de nuestro proveedor de servicios, y mediante sus bases de datos donde tendrá almacenadas las relaciones entre números de teléfono y números de tarjeta, dirigirá la petición al servidor de la entidad de pago adecuada (Euro6000, 4B,..) que a su vez se comunicará con el servidor de comercio correspondiente.

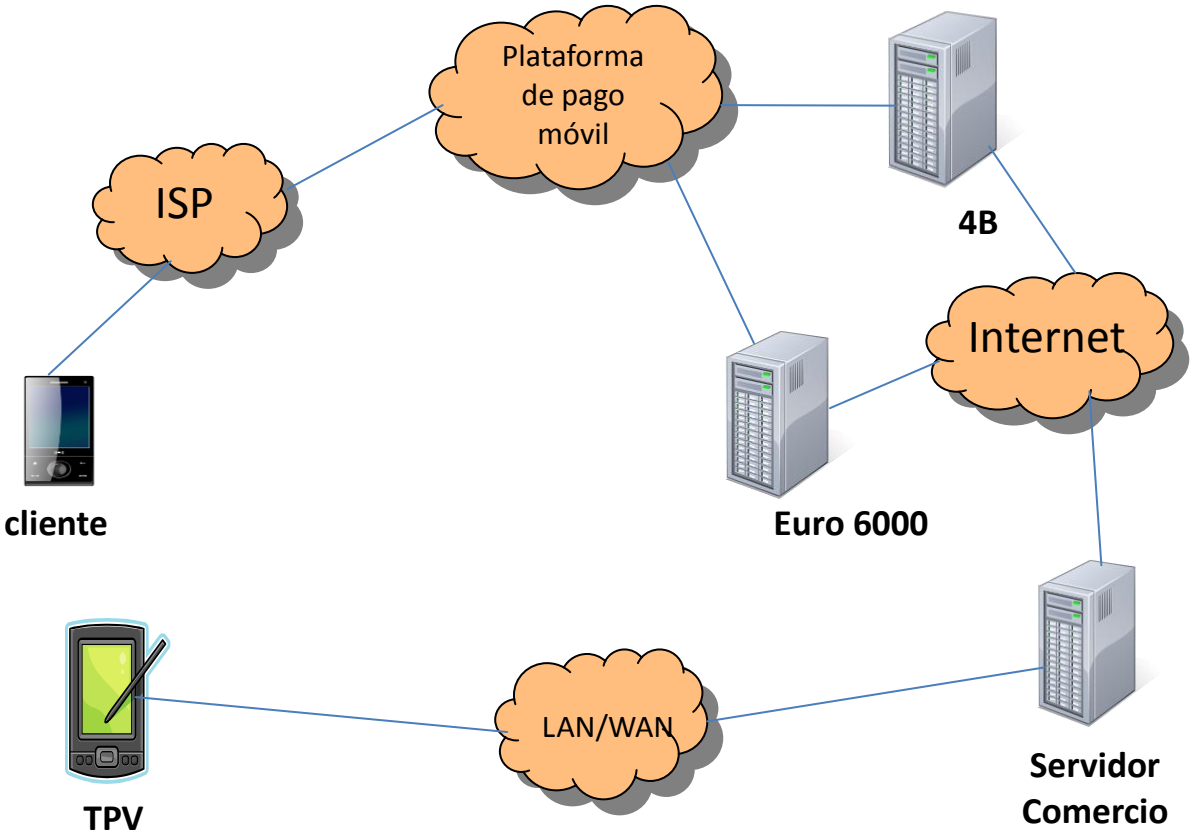

Figura 7.1

Por supuesto, se necesita un proveedor de servicios a través del cual nos podamos comunicar. Dentro del proveedor de servicios, hay un elemento fundamental para los sistemas de pago móvil basados en el servicio sms. El Gateway de SMS, que hace de intermediario entre la operadora móvil y el sistema de pago. Recibe los sms tanto de los usuarios como de los sistemas de pago y los redirige al destinatario adecuado. Normalmente los sms Gateway se encuentran dentro de la red del proveedor de servicios,

pero en algunas ocasiones también se puede encontrar dentro de la red del proveedor de servicios de pago con la única finalidad de poder soportar a varios proveedores de servicio. Básicamente, reciben los sms entrantes por parte de los usuarios y los almacenan en una base datos hasta que pasan a la capa de procesamiento de transacción, y por otra parte reciben los sms que les llegan desde las entidades de pago que nuevamente son almacenados en las bases de datos hasta que se envían a los usuarios finales.

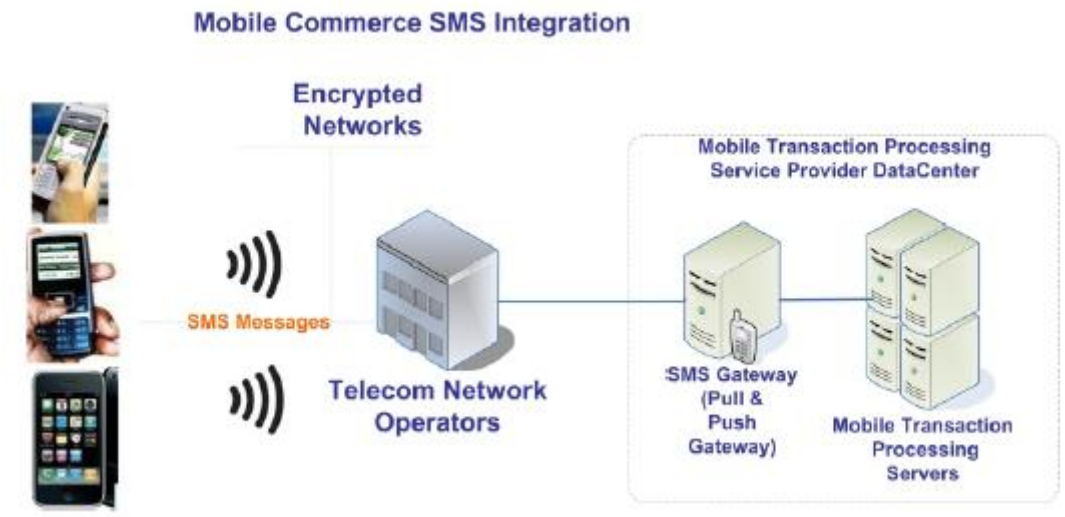

Figura 7.2

Otra de las cosas necesarias para llevar a cabo este sistema de pago mediante el móvil es que el comerciante disponga de un terminal punto de venta (TPV) en su tienda. Este TPV permite acceder al comerciante a la plataforma de pago adecuada y elegir la forma de pago. En muchos casos se aprovechan los datáfonos de los que ya disponía el comerciante con ciertas modificaciones.

7.1.2.-Funcionamiento:

Aunque no existe una solución abierta que obligue a que los pagos por móvil a través de sms sean de una manera determinada, y por tanto, cada plataforma de pago puede tener sus variantes, aquí se va a exponer un modo general de funcionamiento que puede estar sujeto a variaciones dependiendo de quién implemente la solución.

En general la forma de pagar con móvil mediante sms sigue el siguiente procedimiento:

- El comprador le indica al comerciante que desea pagar mediante el móvil.

- El comerciante elige esa opción en el TPV y le pide el número de teléfono al comprador.

- La plataforma de pago correspondiente le envía un sms al usuario indicando la referencia del producto y el coste, y el usuario tendrá que responder el sms introduciendo el NIP (Número de identificación personal).

- Una vez que la plataforma de pago haya recibido la confirmación del pago por parte del usuario, envía la petición de pago hacia la entidad de pago del cliente.

- La entidad de pago del cliente comprueba si es posible realizar la transacción, y si la transacción es posible envía la confirmación tanto a la plataforma de pago como al servidor del comerciante.

- Si todo va bien, al comprador le llegará un sms indicándole que la operación ha sido realizada con éxito, y al TPV también llegará la confirmación de que la transacción se ha realizado.

Normalmente el envío de los mensajes entre el usuario y la plataforma de pago está automatizado mediante una aplicación que reside en el terminal móvil del usuario, ya que una de las ventajas del SMS es que puede interactuar con una aplicación cliente que se encuentre instalada en el móvil. Esta aplicación puede estar almacenada tanto en el terminal móvil como en la SIM. Además, para solventar el problema de que los sms vayan cifrados hasta la misma plataforma de pago sin posibilidad de que nadie pueda ver los mensajes, ni siquiera los propios proveedores de servicios, el cliente se puede instalar un aplicación java en el móvil (PROsms) que le proporcione encriptación punto a punto, con un algoritmo de cifrado simétrico AES-256 y algoritmos Hash SHA-256 para la generación de contraseñas. Al ser un sistema de criptografía simétrica, el cliente necesita ponerse de acuerdo con la plataforma de pago en la clave a utilizar para el cifrado/descifrado de sms.

En el caso de que el cliente no tenga instalada dicha aplicación, los mensajes irían únicamente encriptados en la interfaz radio entre la estación móvil y la estación base. Un punto débil que se puede señalar en este caso es el envío de sms desde el sms-gateway del proveedor de servicios hasta los servidores de la plataforma de pago. En principio esta es una comunicación que puede ser susceptible de algún ataque ya que se produce entre dos redes diferentes y que a priori no tiene por qué estar securizada. El resto de comunicaciones que tiene lugar entre la plataforma de pago móvil y las entidades financieras de los clientes son mediante el protocolo http o con servicios web, pero siempre con la utilización del protocolo SSL para dotar de seguridad a la comunicación, o incluso en muchas ocasiones estas comunicaciones tienen lugar sobre redes privadas administradas directamente por las entidades financieras y los

proveedores de servicios de pago, para evitar que los datos de los clientes viajen por redes de acceso público. Otra opción es crear redes privadas virtuales (VPN) sobre redes públicas para poder comunicarse, pero estas opciones dependen del acuerdo al que lleguen las entidades financieras y las plataformas de pago con móvil, y por lo general es información que no es de dominio público por motivos de seguridad.

Este sistema de pago por móvil ya lleva bastantes años en funcionamiento y de hecho fue de los primeros en implantarse. Como gran ventaja se puede señalar que es de fácil acceso para los usuarios y que no requiere de grandes inversiones ni gastos adicionales, salvo los derivados de las comisiones que pueden conllevar este tipo de pagos. Por otra parte la información bancaria de los usuarios no viaja nunca por redes inseguras, ya que queda registrada dentro de los servidores de las plataformas de pago y cuando el cliente quiere realizar una compra no tiene que facilitar el número de tarjeta sino que tiene que autorizar la transacción facilitando el NIP.

Una de las carencias que se podría destacar respecto a esta forma de pago es que los sms solo serán encriptados desde la estación móvil del usuario hasta la estación base del proveedor de servicios, y en el tramo durante el cual el sms viaja entre el proveedor de servicios y la plataforma de pago móvil el código NIP podría ser interceptado. Sin embargo esta carencia se puede solucionar fácilmente ya que aprovechando las funcionalidades de la tarjeta SIM, se podría desarrollar una pequeña aplicación en Java (client wallet) que permitiese el envio de sms encriptados punto a punto utilizando claves que se podrían almacenar en la propia SIM.

Paymo y Zong, son dos ejemplos de plataformas de pago móvil a través de sms que operan en España.

7.2.-Plataformas de pago con USSD

Las siglas USSD significan Unstructured Supplementary Service Data. Es un protocolo que permite el envío de mensajes cortos de texto, y al igual que el servicio de sms funciona sobre los canales de señalización (SS7) de la red. Es un servicio básico que está presente en los estándares GSM, GPRS y UMTS.

Este protocolo permite establecer un canal más seguro que en el caso de los sms, ya que establece sesiones transaccionales, es decir, es un protocolo orientado a conexión que se encarga de abrir sesiones extremo a extremo permitiendo ejecutar operaciones en tiempo real, a diferencia de sms que utiliza comunicación basada en almacenamiento y reenvío. Este es un detalle importante, porque las plataformas de pago por móvil que opten por esta tecnología son consideradas plataformas online, ya que realizan las operaciones en tiempo real, no como en el caso de los sistemas de pago basados en sms.

Otra de las características que presenta USSD, es que en la parte del operador no solo reside un servidor gateway que almacena y reenvía los mensajes, sino que existe una plataforma que por un lado permite recibir mensajes procedentes de SS7-MAP y por otro ofrece interfaces de aplicación http y xml para terceras partes que quieran implementar servicios a través de USSD, es como si hubiese un back-end y un front-end (figura 7.3). En este caso la plataforma de pago por móvil pertinente conectaría sus servidores mediante los cuales ofrecen el servicio, con la plataforma USSD del proveedor de servicios a través de las interfaces que ofrece este último.

Las interfaces que se puedan ofrecer, y los servicios que se pueden soportar e integrar con USSD dependen mucho del proveedor de servicios y de la lógica que tenga implementada en su plataforma USSD, por tanto es un factor que tendrá que negociar la plataforma de pago que quiera desplegar su servicio, y precisamente en estos puntos de negociación es

dónde se pueden llegar a establecer las comisiones finales que se aplicarán a la compra del producto e impactarán en el consumidor final.

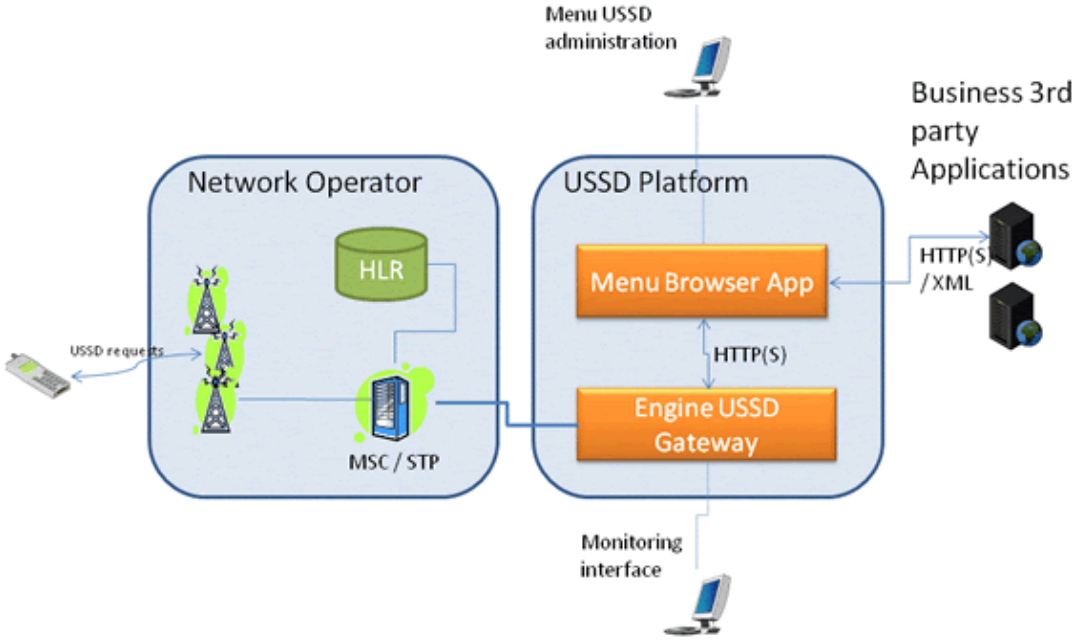

Figura 7.3

7.2.1.-Arquitectura:

Usuario con terminal móvil. Obviamente el terminal móvil es el elemento fundamental alrededor del cual gira el método de pago. El usuario tendrá que disponer de un terminal de telefonía móvil y en principio no necesita albergar ninguna información adicional en su móvil. No tiene que instalar ningún software adicional, ni guardar información bancaria dentro de su tarjeta SIM. Con simplemente disponer de un terminal móvil y darse de alta en la plataforma de pago por móvil, asociando las tarjetas de crédito que el usuario desee, es suficiente para poder empezar a utilizar el servicio. En una de las variantes de funcionamiento sobre USSD, cuando un usuario contrata el servicio de pago con móvil, se le asigna un código de barras PAN en un adhesivo para pegar en su teléfono. Esta variante se utiliza para pagos presenciales en la tienda como se verá más adelante.

La plataforma de pago por móvil. Otro de los elementos clave para poder desarrollar este sistema de pago con móvil. Nuevamente su función es interactuar con las entidades de pago correspondientes, pero en este caso la manera en que se comunica con el proveedor de servicios varía con respecto al sistema de pago basado en sms. En este caso la plataforma de pago se comunicará a través de interfaces de http y xml con la plataforma ussd, pudiendo establecer una comunicación directa desde su aplicación de procesamiento de pagos con el usuario final a través del proveedor de servicios.

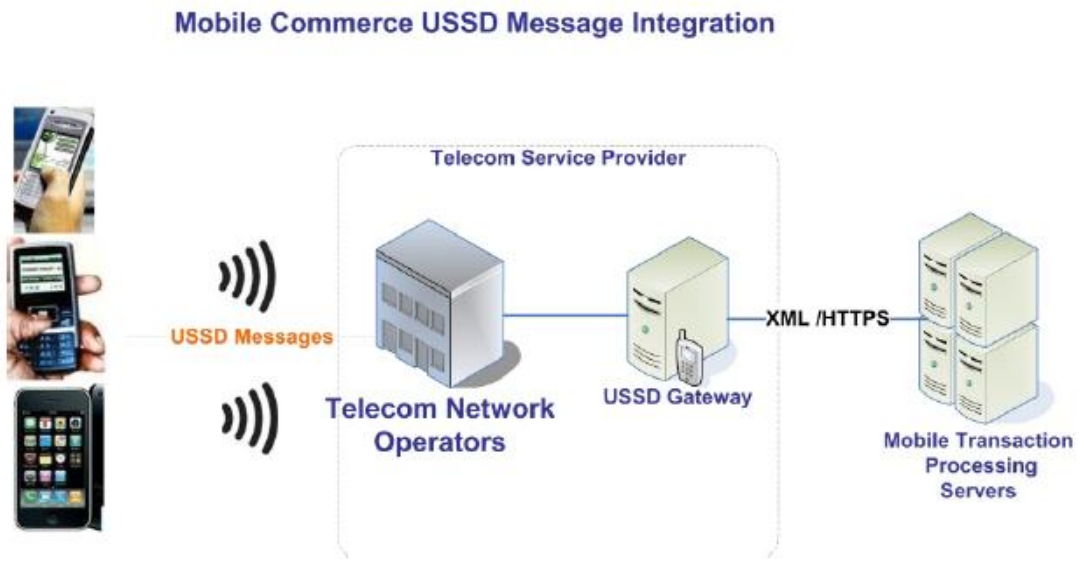

Figura 7.4

Terminal Punto De Venta. Al igual que en el caso del sistema de pago por sms, es necesario que el comerciante disponga de un terminal punto de venta para poder llevar a cabo la transacción de compra, utilizándolo para iniciar la transacción de compra o para recibir la confirmación de que la transacción ha sido realizada correctamente y poder generar el ticket de compra. Al igual que en el caso anterior, estos TPV pueden ser datáfonos con pequeñas adaptaciones.

7.2.2.-Funcionamiento:

Principalmente, las plataformas de pago con móvil que operan con el protocolo USSD tienen dos modos de funcionamiento. Uno presencial y otro no presencial. El modo no presencial también es conocido como pago por referencia. A continuación se detallan los dos:

- *Modo no presencial:*

- El usuario es quien inicia la petición de compra introduciendo un código en su terminal móvil que consta de un número relacionado con la plataforma de pago más el número de referencia que se le designa al producto en cuestión. **145*1*REF#.*

- La referencia se manda mediante el protocolo USSD y llega hasta la plataforma USSD del proveedor de servicios. En función del código USSD, esta petición se comunica con el servidor pertinente de la plataforma de pago móvil.

- El servidor de la plataforma de pago móvil contiene lo que se denomina un gestor de referencias, que se encarga de averiguar a qué comercio corresponde la referencia introducida por el consumidor. Algunos gestores de referencia contienen toda la información sobre los productos con lo que operan, sin embargo también existe la posibilidad de que el gestor de referencias no disponga de la referencia de todos los productos y tengan que hacer una consulta al servidor del cliente, lo cual es una ventaja para el cliente, ya que cada vez que quiera añadir un nuevo producto no tendrá que mandar actualizar el gestor de referencias.

- Una vez localizado el producto, se envían los datos finales de la compra al cliente, para que este los pueda verificar y validar mediante el NIP.

- La plataforma de pago una vez que recibe la confirmación de pago por parte del cliente encamina la petición a la entidad de pago correspondiente, teniendo en cuenta la tarjeta bancaria asociada del cliente.

- La entidad de pago comprobará si la transacción se puede llevar a cabo, y en caso afirmativo se informa al servidor del comercio de la transacción pidiéndole la confirmación de los datos de compra y la asignación de un número denominado localizador con el cual el cliente pueda ir a recoger el producto al establecimiento.

- Dependiendo de la entidad de compra, la transacción se da por finalizada o se deja en estado de precompra, confirmándola el comercio cuando el cliente vaya a recoger el producto.

➢ *Modo presencial:*

El modo de pago presencial tiene prácticamente el mismo modo de funcionamiento que el no presencial. La principal diferencia es que el usuario no es quien inicia la petición de compra sino que lo hace el comerciante a través del TPV. Para iniciar la petición de compra a través de la plataforma móvil tiene dos opciones, o leer el código de barras PAN que lleva pegado el consumidor en su terminal móvil, o introducir el número de teléfono móvil del abonado. Asimismo al cliente le llegará al móvil la petición de confirmación donde tendrá que facilitar el NIP para autorizar la transacción. Si la operación se autoriza, tanto la entidad

financiera del comprador como la del vendedor reciben la confirmación al mismo tiempo. Y en este caso no se asignan localizadores, sino que tanto comerciante como consumidor reciben la confirmación de que la transacción ha sido realizada.

En esta plataforma no tenemos el "vacío" de seguridad con el que nos encontrábamos en el caso de los sms, ya que el intercambio de información que tiene lugar entre el Gateway USSD del proveedor de servicios y la plataforma de pago con móvil, va sobre comunicaciones cifradas con el protocolo SSL, al igual que pasa entre las conexiones existes que tienen lugar entre las entidades financieras de los clientes y las plataformas de pago móvil, que en algunas ocasiones incluso se establecen en redes privadas o sobre VPNs.

Esta tecnología es un poco más segura que en el caso de los sms, ya que la comunicación que establece el usuario con la plataforma de pago está protegida todo el tiempo. Además tiene la ventaja respecto a los sms de que se trata de una comunicación orientada a conexión, por lo que se evitan pérdidas y desorden de mensajes. Cuando el usuario se dispone a comprar un producto tiene que facilitar el NIP a través de un mensaje ussd que irá encriptado hasta el Gateway ussd y desde allí se comunicará con la plataforma de pago pertinente a través de conexiones seguras, SSL, https…dependiendo de la conexión que hayan acordado entre el proveedor de servicios y la plataforma de pago. Una vez la información llega a la plataforma de pago es esta quien se encarga de gestionar los pagos entre las diferentes instituciones financieras dentro de redes seguras. La información bancaria del cliente únicamente viaja por estas redes seguras, ya que cuando el cliente se da de alta en la plataforma de pago tiene que asociar un número de tarjeta que estará guardado en los servidores de la plataforma de pago y que el usuario no tendrá que facilitar vía ussd, únicamente tendrá que facilitar su NIP el cual irá encriptado hasta que llegue al gateway ussd.

Esta tecnología también fue usada en las primeras plataformas de pago. Actualmente está prácticamente en desuso al igual que las plataformas de pago basadas en el servicio sms. Como ventajas frente a los sistemas basados en sms podemos destacar que es más rápido, no hay pérdida ni duplicados de mensajes ya que es un protocolo orientado a conexión, y es más barato, el precio de la realización de una transacción es mucho más barato que el envío de un sms. Como desventaja se puede señalar que las aplicaciones que utiliza USSD se encuentran alojadas en un servidor, pero estas aplicaciones no tienen la capacidad de poder interactuar con otra aplicación que se encuentre en el terminal móvil. Además USSD no es adecuado para contextos donde se necesite obtener información del terminal móvil para poder completar una transacción.

Respecto a la seguridad, es un protocolo que se muestra más seguro que el servicio de sms, ya que es orientado a conexión. Pero por sí mismo USSD no ofrece seguridad adicional a parte de la encriptación que ofrece GSM entre la estación móvil y la estación base. Por lo que si se quisiese ofrecer una encriptación punto a punto habría que desarrollar una aplicación para ofrecer ese servicio.

Mobipay es un ejemplo de plataforma de pago móvil que operaba en España usando el protocolo USSD.

7.3.-Plataforma de pago con WAP

Las siglas de WAP significan (Wireless Application Protocol). Se trata de un conjunto de protocolos y un entorno de aplicación para el desarrollo de servicios y contenidos accesibles desde los terminales móviles. Fue creado con la finalidad de dotar a los dispositivos móviles de servicios avanzados de datos a través de los cuales pudiese acceder a contenidos y servicios de internet.

Gracias a la llegada de GPRS (General Packet Radio Services), que es una tecnología de conmutación de paquetes, las redes de comunicaciones móviles mejoraron notablemente sus prestaciones en la velocidad y acceso a servicios de datos de internet y por consiguiente WAP también mejoró sus prestaciones.

WAP fue la primera plataforma que permitió el acceso a internet desde los terminales móviles, y aunque con el tiempo fue mejorando en prestaciones, fue una plataforma que se adaptó a las limitaciones del entorno inalámbrico. Por un lado los móviles contemporáneos de WAP tenían pantallas más pequeñas comparadas con las de ahora, menos capacidad de procesamiento y menos cantidad de memoria, y por otro lado, las redes de telefonía móvil antes de la llegada de UMTS mostraban limitaciones de velocidad, latencia y estabilidad.

En el año 1998 apareció la primera versión de WAP, y luego se fueron desarrollando sucesivas versiones que se iban adaptando a los cambios en el mercado y a las nuevas tecnologías en redes y terminales, hasta la llegada definitiva de WAP 2.0 que soporta la arquitectura estándar de protocolos de internet con ligeras variantes que se adaptaban a internet con la tecnología proxy.

De cara a los sistemas de pago con móvil, la aparición de una tecnología que permitía el acceso a internet desde el terminal móvil, supuso una revolución total. No hay que olvidarse que internet es el núcleo alrededor

del cual se desarrolla el comercio electrónico, y con la aparición de WAP se facilitaba el acceso al comercio electrónico desde el terminal móvil con ciertas modificaciones respecto a internet para optimizar el funcionamiento.

Pero no todo son ventajas, ya que el hecho de que se pueda acceder a internet desde el móvil implica que hay que adoptar los mecanismos de seguridad existentes en internet para evitar posibles ataques.

Otra de las cosas que cambia totalmente es la arquitectura del sistema de pago con móvil, porque ya no es necesaria la existencia de una plataforma de pago móvil en sí. Teniendo acceso a internet desde el móvil, podemos acceder a los servidores WAP del comercio desde donde podremos pagar con tarjeta de crédito los productos que deseemos.

7.3.1.-Arquitectura:

La arquitectura de WAP 2.0 sigue el modelo www. Cuenta por un lado con un cliente WAP integrado en el terminal móvil, que es básicamente un navegador, y por otro lado se encuentra el servidor WAP donde se encuentra almacenada la información y los servicios.

Por tanto, por parte del cliente se requiere un terminal móvil con acceso a redes GPRS y con un navegador WAP integrado, a través del cual pueda acceder a los servidores de comercio electrónico donde pueda efectuar sus compras.

Los servidores WAP pueden guardar información en varios formatos estándar diferentes (JavaScript, html, jpeg…) y también puede generar contenidos interactivos y dinámicos utilizando tecnologías CGI, PHP, Servlets, etc. Estos servidores contienen una variedad muy grande de información, desde servicios de noticias que pueden ofrecer los proveedores de servicios, hasta servicios de compras de entradas para el

cine, y normalmente se encuentran alojados dentro de la red del proveedor de servicios.

Para establecer la comunicación entre el cliente y el servidor WAP se utilizan los protocolos estándares de internet: ip, tcp, http, pero como se ha indicado anteriormente, estos protocolos han sido adaptados para poder ser usados en el entorno inalámbrico. Esta adaptación se lleva a cabo a través de la tecnología proxy, que consiste en colocar un Gateway en el medio de la comunicación que tiene lugar para comunicar dos entornos que utilizan protocolos distintos donde es necesaria su traducción.

Desde el terminal móvil se inicia una comunicación WAP hacia un gateway, utilizando el servicio portador GPRS, y se implementan los protocolos WP-http, WP-tcp y WP-ip que son adaptaciones de los protocolos estándar de internet que ayudan a mejorar las prestaciones y la eficiencia de las redes móviles, ya que presentan características muy diferentes como pueden ser la probabilidad de error o el ancho de banda. Pero si estamos hablando de que vamos a utilizar la tecnología WAP para realizar compras desde el móvil, hay que proporcionar la seguridad adecuada a la comunicación. Como en internet el protocolo estrella para proporcionar comunicaciones seguras es SSL, lo que aquí se utiliza es una adaptación de SSL llamada WTLS. Como ya sabemos SSL utiliza una combinación de la criptografía simétrica y asimétrica, negociando una clave simétrica para la sesión mediante el uso de criptografía asimétrica. Como SSL fue diseñado teniendo en cuenta comunicaciones entre PC´s y servidores, la capacidad de procesamiento necesaria para implementar los mecanismos criptográficos no era un problema. Sin embargo, en los terminales móviles, aunque cada vez se asemejan más a los PC´s, la capacidad de procesamiento puede llegar a suponer una importante barrera. Es por esta razón que se utiliza la adaptación del protocolo SSL llamada WTLS para entornos WAP.

El proxy WAP instalado entre la red móvil e internet, implementa por un lado estos protocolos que acabamos de ver, y por otro los protocolos

estándar de internet, haciendo posible el acceso a servicios de internet desde un terminal móvil.

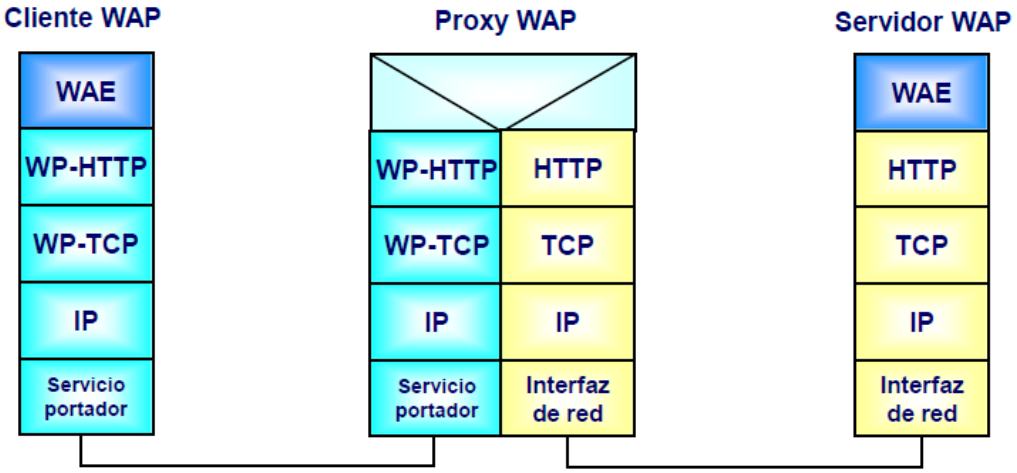

Figura 7.5

El proxy WAP se encarga de traducir los protocolos y permite el establecimiento de un túnel orientado a conexión entre el cliente y el servidor WAP, proporcionando seguridad extremo a extremo independientemente del servicio portador que sea usado, GPRS, UMTS…

La utilización del gateway como traductor de protocolos, puede dar lugar a pensar que es un punto débil en la comunicación desde el punto de vista de la seguridad, debido a que se puede pensar que al realizar la traducción del protocolo WTLS a SSL/TLS hay que desencriptar la información en algún momento y se puede acceder a ella. Sin embargo, el proceso de encriptación y desencriptación tiene lugar bajo unos parámetros de seguridad optimizados en velocidad de manera que el contenido original sea borrado de la memoria volátil del gateway tan pronto como sea posible, restringiendo al mismo tiempo el acceso físico al gateway.

7.3.2.-Funcionamiento:

Gracias a que con la utilización de WAP podemos acceder a internet, podemos hacer uso desde el móvil de los sistemas de pago ya existentes, como por ejemplo Paypal.

Para pagar desde el móvil con Paypal necesitamos estar dados de alta en el sistema Paypal y disponer de un terminal con un navegador WAP. La transacción se desarrolla de la siguiente manera:

El cliente accede mediante el móvil al portal web del vendedor, donde puede ver los productos disponibles para comprar.

Una vez el cliente ha elegido el producto que desea comprar lo selecciona, y el vendedor muestra a través de su web la opción de compra mediante Paypal.

Cuando el cliente selecciona esta opción, el vendedor se pone en contacto con el servidor de Paypal, normalmente utilizando servicios web, para solicitar el inicio de transacción. En la petición de inicio de transacción incluye información sobre el pedido del cliente, información sobre el flujo de Paypal que incluye URL de devolución y URL de cancelación, y de forma opcional también puede llevar información sobre el cliente, nombre, número de teléfono, etc.

El servidor de Paypal devuelve una respuesta que contiene un código personal que identifica la transacción (token), y el vendedor redirige al cliente a la URL de Paypal con el código personal adjunto. Cuando se produce esta redirección es como si el cliente se tuviese que conectar de nuevo, pero en este caso tiene que iniciar una conexión segura con los servidores de Paypal. Es decir, cuando se establece la conexión entre los servidores de Paypal y el cliente móvil tiene que ser bajo una conexión segura, que en este caso es llevada a cabo mediante SSL, y además de los parámetros de seguridad que negocia SSL para establecer una sesión, en este caso Paypal añade uno nuevo que es el token para tener identificada

en todo momento la trasacción. Toda la información intercambiada entre el cliente y el servidor de Paypal se produce a través de http securizado con SSL. En este sistema de pago tampoco es necesario enviar los datos bancarios del usuario por la red pública, únicamente es necesario autenticarse dentro de Paypal y autorizar la transacción con un PIN.

Se inicia el flujo entre el servidor de Paypal y el cliente. Primero el cliente tiene que iniciar sesión en la plataforma Paypal facilitando su correo electrónico y contraseña. Una vez activado, confirma los detalles de la compra introduciendo su número de teléfono y un PIN.

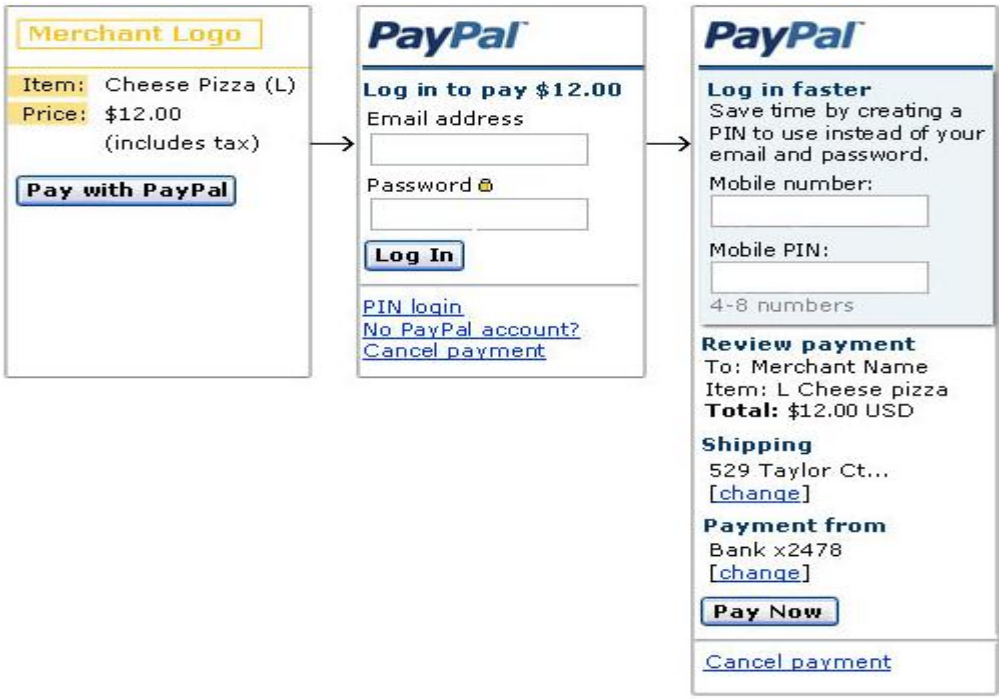

Figura 7.6

Una vez confirmados los datos por parte del cliente, Paypal se encarga de realizar las transacciones correspondientes, y en el caso de que todo vaya bien, muestra una página de confirmación del pedido y además envía la información de compra al correo electrónico del cliente.

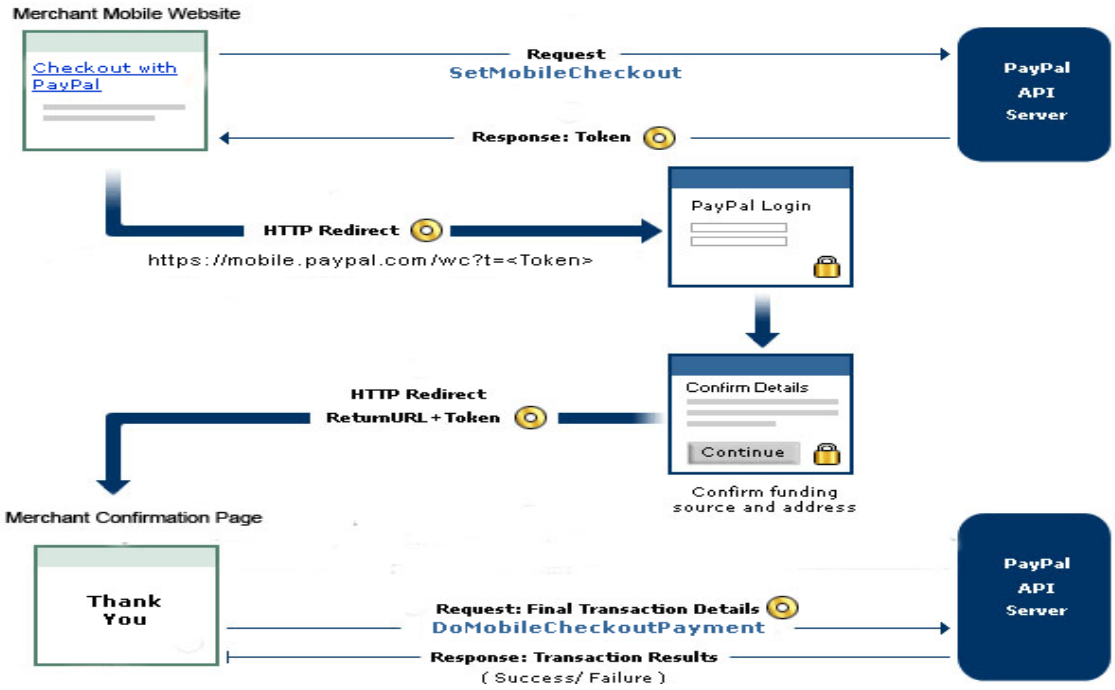

Figura 7.7

Este método de pago todavía es usado por algunos usuarios, aunque hoy en día con las velocidades que nos ofrecen las redes UMTS cada vez son menos los que optan por esta tecnología.

Las principales desventajas de utilizar WAP para acceder a internet son, la limitación de velocidad de acceso y la problemática de encontrar servidores WAP con contenidos y servicios disponibles que se vayan actualizando, ya que la mayoría de los usuarios hoy en día opta por la utilización de smartphones con capacidades de velocidad mayores.

Además, en este caso particular de utilización de Paypal como medio de pago, cabe la posibilidad de ataques de phising por medio de enlaces fraudulentos que le puedan llegar al usuario en los e-mails.

7.4.-Plataformas de pago con aplicaciones (app)

La llegada de la tecnología UMTS (3G) a las redes de comunicaciones móviles supuso una mejora muy considerable de las prestaciones de la red, y bajo mi punto de vista, el impulso definitivo para que la utilización de los terminales móviles se convirtiese en algo esencial en nuestro día a día por la cantidad de información y servicios a los cuales se puede acceder.

Entre las mejoras más destacables que supuso la llegada de la tecnología UMTS están, aumentar la capacidad para dar servicio a una alta densidad de usuarios, poder asignar dinámicamente el ancho de banda, ser una tecnología compatible para una amplia gama de terminales, y poder integrar protocolos IP en el terminal ya que UMTS es una tecnología que utiliza conmutación de paquetes.

Otra de las características más importantes aportadas por la tecnología UMTS, y más valorada por los usuarios, fue el aumento de tasas de transferencia permitiendo mayores velocidades para poder descargarse datos o utilizar servicios multimedia. Esta capacidad incluso se ha visto mejorada con la nueva evolución de UMTS, que es considerada la 3,75G y es conocida como HSDPA/HSUPA, que fundamentalmente aportan un aumento considerable de las velocidades de subida y bajada de datos tanto en el canal ascendente como descendente, en concreto, aumentan entre 4 o 5 veces la velocidad de descarga de datos permitiendo tasas de transmisión que van desde 1 hasta 1,4Mbps, consiguiendo además reducir el tiempo de latencia del enlace.

Gracias a estas y otras mejoras, los usuarios hacen más uso de las redes de comunicaciones móviles ya que tienen al alcance poder acceder desde su terminal móvil a información y servicios con unos tiempos aceptables que antes solo podían consultar desde un PC.

También hay que decir que las mejoras en las redes de comunicaciones móviles han venido acompañadas en paralelo de una impresionante

evolución de los terminales móviles. De otra forma, no sería posible la utilización de los nuevos servicios que nos ofrecen las redes si no dispusiésemos de los terminales con la tecnología adecuada para poder usarlos.

Los terminales móviles han evolucionado hasta lo que conocemos hoy en día como teléfonos inteligentes (smartphones), proporcionándonos mayores capacidades de procesamiento y de conectividad, permitiéndonos el uso de los servicios disponibles de las redes móviles. Realmente son como miniordenadores que nos permiten ejecutar casi cualquier tipo de tarea que pudiésemos realizar con un PC.

Esta evolución tecnológica de los terminales móviles ha proporcionado también un desarrollo considerable en cuanto al software que utilizan. Actualmente los smartphones utilizan sistemas operativos más complejos y avanzados que permiten la ejecución de múltiples tareas, la implementación de protocolos IP y el desarrollo de múltiples aplicaciones. Existe toda una industria de software dedicada a la creación y desarrollo de sistemas operativos para móviles, donde los que más destacan son Android que pertenece a Google e IOS que es el sistema operativo que llevan integrado los iPhone de Apple. A su vez, estos sistemas operativos soportan una gran cantidad de aplicaciones que son desarrolladas para dar diferentes servicios que pueden ir desde el ocio hasta el m-commerce.

El gran inconveniente de estas aplicaciones es que no son multiplataforma, es decir, que según en qué sistema operativo vayan a funcionar tienen que ser desarrolladas a partir de un API específico facilitado por la plataforma móvil.

Las aplicaciones monedero, también conocidas como e-wallet son un ejemplo de estas aplicaciones, que ya vimos que existían para PC, que surgen como resultado de las nuevas prestaciones de las redes móviles y el avance tecnológico de los terminales.

Aquí vamos a ver el caso particular de la aplicación GoogleCheckout para móvil.

7.4.1.-Arquitectura:

Para poder utilizar este sistema de pago, el usuario necesita disponer de un Smartphone con un sistema operativo que soporte la aplicación GoogleCheckout. Además también deberá disponer en el Smartphone de un navegador web (micronavegador) que le permita acceder a la página web del comerciante.

Estos navegadores desarrollados específicamente para S.O de smartphones, pueden reproducir perfectamente el contenido de los portales comerciales soportando la gran mayoría de estándares web, html 5.0, css 3.0…., lo cual permite al usuario acceder desde su móvil al contenido completo que pueda mostrar el comerciante en la web, como si estuviese accediendo desde el PC de su casa.

EL proveedor de servicios cuenta dentro de su red de acceso móvil a internet con un servidor adaptador de contenidos, que cuando detecta que se ha realizado una petición para acceder a una página web desde un terminal móvil se encargará de adaptar el contenido que devuelva el servidor web para que pueda ser reproducido en el terminal móvil del usuario adaptándose a sus limitaciones.

El comerciante tendrá que disponer de un portal web donde oferte sus productos y un acuerdo con la empresa que implemente la aplicación de pago para poder comprar sus productos, en este caso GoogleCheckout.

En este caso la empresa propietaria de la aplicación de pago actúa como intermediaria entre el comprador y el vendedor y se encarga de las transacciones necesarias para realizar el pago, por tanto tendrá que disponer de un servidor que se encargue de mantener las comunicaciones necesarias con la entidad financiera del comerciante y con la compañía de la tarjeta del cliente.

Dado que cada vez hay más empresas que se apuntan al negocio del comercio móvil, desarrollando sus propios sistemas de pago, existen

terceras partes que se encargan de integrar "payment gateways" para actuar de intermediarios haciendo posible la integración entre múltiples sistemas de pago que utilizan diferentes soluciones como WebServices, simples protocolos de transferencia de ficheros seguros, etc.

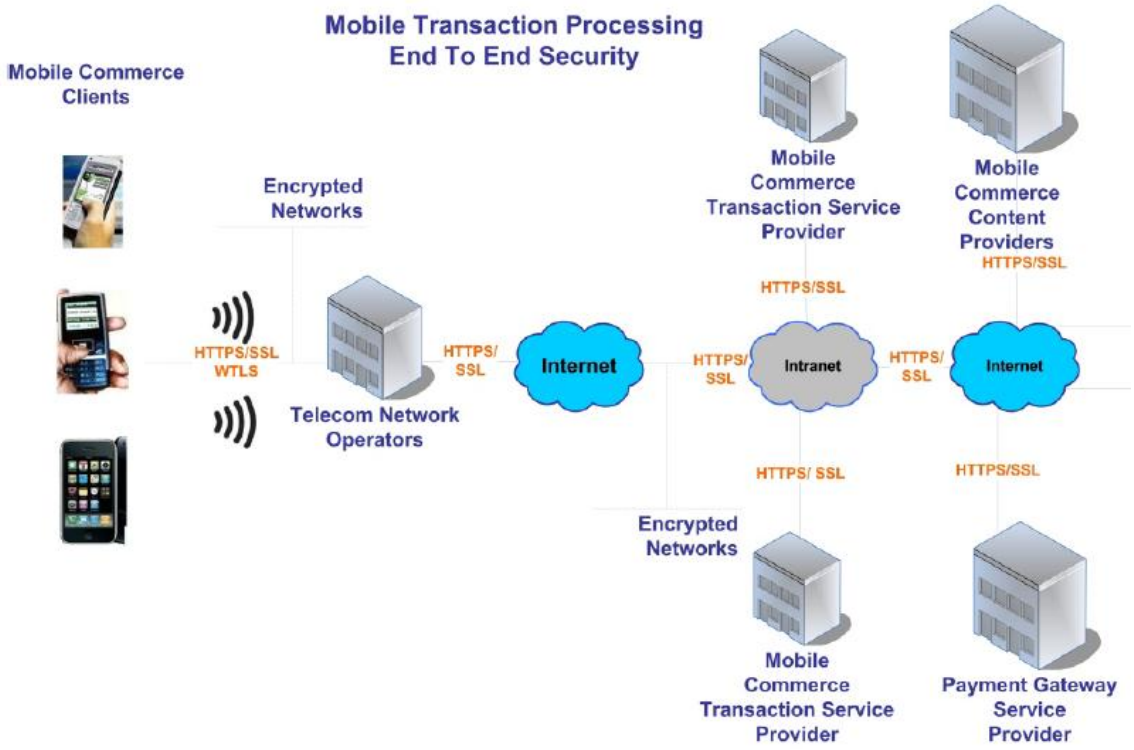

Figura 7.8

7.4.2.-Funcionamiento:

El comprador accede a la página Web del comerciante y elige el producto que desea comprar.

Una vez el cliente ha elegido el producto, elige la opción de pago GoogleCheckOut. Si el cliente accede por primera tendrá que darse de alta en la aplicación facilitando un nombre de usuario, contraseña y demás datos personales, entre los que se encuentran los datos bancarios. Lo bueno de este sistema de pago es que los datos bancarios solo se introducen una vez cuando el usuario se da de alta en el sistema. A partir de ese momento los datos quedan almacenados en el servidor de la aplicación debidamente encriptados y cuando el usuario acceda a la plataforma bastará con que facilite su nombre de usuario y contraseña para efectuar la compra. Es un sistema de pago muy similar al utilizado por Paypal.

Una vez dentro de la plataforma de pago, el cliente confirma los datos de la compra y procede a aprobar la transacción, por lo que en este caso GoogleCheckout procede a realizar la transferencia de dinero desde la cuenta del cliente al banco del comerciante.

Googlecheckout no soporta el protocolo 3D-Secure para realizar los pagos, pero las comunicaciones que tienen lugar entre Googlecheckout y las diferentes instituciones financieras son establecidas mediante sesiones encriptadas SSL como se puede apreciar en la figura 7.8, o bien bajo redes privadas o VPNs, pero este tipo de comunicaciones siempre están debidamente protegidas debido a la importancia de la información que intercambian.

Si la compra se realiza correctamente, GoogleCheckout informa tanto al cliente como al comerciante de que la transacción se ha realizado correctamente.

Otra forma de utilizar GoogleCheckout es acceder directamente desde la aplicación de la que se dispone en el móvil al store de Google, donde los servidores de google pueden mostrar diferentes productos que tienen a la venta de los diferentes fabricantes con los que mantienen acuerdo. Por supuesto esta primera comunicación que se establece con los servidores de Google se realiza de forma segura, conectándose a través de https. Una vez el cliente elige el producto que desee, simplemente se tiene que autenticar con su contraseña para poder validar la compra. Una vez que el usuario apruebe la compra Google verifica los datos y si todo es correcto se encarga de efectuar la compra cargando el importe necesario en la tarjeta del cliente y realizando la transferencia de dinero hacia el banco del comerciante.

Los modos de pago que acepta GoogleCheckout son Visa y MasterCard. Por tanto al darse de alta en la plataforma hay que facilitar los datos de la tarjeta de crédito. Los pagos realizados pueden son cargados directamente a la tarjeta que se haya vinculado a la cuenta.

Como se ha indicado antes, la fortaleza de este sistema reside en que los datos financieros solo son introducidos una sola vez y el servicio oculta el número de tarjeta del usuario. Estos datos pueden ser almacenados tanto en el servidor de la aplicación (“la nube”), como en el terminal móvil debidamente encriptados dentro de la aplicación.

Como ventajas de este sistema de pago se puede destacar que es gratuito para el cliente, aunque no así para el comerciante, que está muy extendido, pese a su reciente aparición fuera de EE.UU, por lo que goza de una alta disponibilidad para realizar compras, y además esta aplicación mantiene un historial de compras donde se podrán revisar pedidos anteriores y consultar todos los detalles de compras anteriores. Se puede señalar como desventaja que es un medio de pago que está prohibido dentro del gran portal de compras por internet que es eBay, debido a que ebay es propietaria del sistema de pago Paypal.

Otra de las soluciones de pago con móvil que está teniendo relativo éxito y también se fundamenta en la existencia de una aplicación en el móvil, es el sistema QR-Code. QR- Code son las siglas de Quick Response Barcode, y se trata de un sistema que almacena información en una matriz de puntos o un código de barras bidimensional creado por la compañía Japonesa Denso-Wave.

El sistema de pago mediante esta tecnología consiste en disponer de una aplicación en el móvil que será facilitada por un comercio en concreto, donde el cliente se registrará y asociará una tarjeta para poder realizar los pagos. Cuando el cliente desee realizar un compra accederá a la aplicación, elegirá el producto que desee comprar y una vez lo hay elegido, la aplicación le mostrará un código como el que se puede ver en la figura 7.9 que contendrá toda la información sobre el producto (QR-Code), y para finalizar la operación de pago este código tendrá que ser leído por un lector de códigos ubicado en el local comercial.

Figura 7.9

7.5.-Plataformas de pago con NFC

Esta parece ser la tecnología definitiva para afianzar los pagos con móvil. NFC son las siglas de Near Field Contact. Es una tecnología de comunicación inalámbrica que permite intercambiar datos entre dos dispositivos próximos, situados a pocos centímetros siguiendo el estándar ISO 14443 y trabajando en la banda de 13,56Mhz. Esta tecnología establece conexión wireless entre las aplicaciones de la red y los dispositivos electrónicos y como funciona en la banda de 13,56Mhz no está sujeta a ninguna restricción ni licencia de uso, pero por contra el alcance de funcionamiento debe ser de 20cm o menos, lo que obliga a las aplicaciones que se usen a estar próximas entre sí.

Existe un estándar para NFC que es el NFCIP-1, y que soporta dos modos de funcionamiento:

- *Activo:* ambos dispositivos generan su propio campo electromagnético, que utilizarán para establecer la mantener la comunicación.
- *Pasivo:* uno de los dispositivos genera el campo electromagnético, y el otro se aprovecha de la modulación de la carga para transferir los *datos.*

Además este estándar permite funcionar a diversas velocidades 106,212 o 424Kbit/s. Estas velocidades son negociables entre los dispositivos dependiendo del entorno en el que trabajen y se puede reajustar la velocidad en cualquier instante de la comunicación.

El problema para poder desplegar este sistema de pago con móvil es que es indispensables que haya desplegada una infraestructura de sensores por parte de los comerciantes. Normalmente estos sensores se pueden integrar en los propios datafonos o adquirir nuevos TPV que dispongan de

sensor NFC nativo. Por lo tanto vemos que este es un sistema de pago donde, como los primeros que hemos visto, es necesario que el comerciante disponga de un TPV.

Este sistema de pago se antoja muy práctico para realizar compras con importes pequeños y en establecimientos grandes, donde hay que esperar grandes colas para poder realizar el pago. Con este sistema de pago con móvil se puede tardar menos de un segundo en cobrar, gracias a que no se realiza una transacción remota sino que se está debitando un chip de prepago.

7.5.1.-Arquitectura:

Para poder realizar los pagos con la tecnología NFC desde el terminal móvil, es necesario que el móvil incorpore nativamente la tecnología NFC, que básicamente consiste en un chip, o también existe la posibilidad de que este chip sea incorporado al teléfono mediante una tarjeta de memoria externa o la propia SIM.

Además de disponer del chip NFC el terminal móvil deberá disponer de una aplicación que le permita ejecutar el con la tecnología NFC.

El comerciante debe disponer de un terminal de venta virtual TPV que implemente la tecnología NFC y le permita al cliente realizar el pago mediante ese método.

El cliente tendrá vinculados a la aplicación NFC los datos de la tarjeta de crédito, y una vez se efectúe la comunicación entre el terminal móvil y el TPV, el resto de la infraestructura de pago funcionaría igual que cuando un usuario se dispone a efectuar un pago con tarjeta mediante datáfono.

La diferencia principal estriba en que la transacción es asíncrona, es decir, una vez que el TPV del comerciante recibe los datos bancarios del cliente a través del protocolo NFC, no realiza la comunicación con la entidad bancaria en el mismo momento sino que almacena la petición y efectúa la transacción más tarde, haciendo que el pago sea mucho más rápido y ágil.

7.5.2.-Funcionamiento:

El pago con terminal móvil mediante tecnología NFC permite muchas variantes de uso. Para empezar, como se ha indicado anteriormente, el chip NFC puede venir integrado nativamente en móvil o por el contrario se puede añadir mediante una tarjeta SIM que soporte esa funcionalidad, o mediante una tarjeta de memoria externa.

El usuario tiene que vincular la información de las tarjetas de crédito a la aplicación correspondiente. Esta información siempre va a residir en el terminal móvil, bien sea en la tarjeta SIM debidamente encriptada, en la memoria interna del teléfono, lo cual sería una solución poco segura ante un posible robo del terminal, o también se puede guardar la información en una tarjeta de memoria externa que incluya la aplicación NFC y permita la encriptación de la información de la tarjeta.

La aplicación NFC para efectuar la compra, puede ser una aplicación desarrollada para un Smartphone según el sistema operativo que use, pero también, como se ha mencionado antes, existen soluciones que integran dentro de una tarjeta de memoria la aplicación con el chip NFC sin necesidad de disponer de un terminal que tenga chip NFC o capaz de soportar una aplicación con interfaz gráfica como la de los Smartphone.

Por ejemplo las compañías Visa y DeviceFidelity han desarrollado una solución como esta, denominada In2Pay:

Figura 7.10

La forma de iniciar la comunicación para efectuar el cambio también puede variar. Por un lado podemos utilizar aplicaciones que nos permiten acceder a una tienda virtual donde seleccionamos los productos que deseamos pagar y después simplemente acercamos el móvil al TPV para confirmar la compra. Otra opción es que el TPV del comerciante sea quien inicie la comunicación NFC con el terminal móvil indicando los productos que se van a comprar y el importe total. El cliente solo tendrá que confirmar los datos de compra e introducir un PIN para validar la transacción. Este paso siempre es necesario por motivos de seguridad se obliga al cliente a introducir un PIN antes de aprobar una compra.

Por supuesto, la información que viaja entre el terminal móvil y el TPV durante la comunicación NFC viaja encriptada.

Una vez que el usuario ha confirmado la petición de compra, la comunicación con la entidad bancaria no se realiza inmediatamente en el momento de pago, sino que periódicamente se lanza un proceso que realiza todas las transacciones asociadas a los débitos realizados.

La principal dificultad de implementar este sistema de pago reside en desarrollar las aplicaciones necesarias para que el usuario pueda seleccionar esa forma de pago y que el comerciante también ponga a disposición del consumidor un posible entorno donde pueda seleccionar los productos antes de efectuar el pago. La forma de pago es muy parecida a la que actualmente existe en los comercios, ya que la principal diferencia es que en lugar de tener que pasar una tarjeta de crédito por un lector, y esperar a que la transacción sea validada, simplemente hay que acercar el teléfono móvil a un TPV y validar la compra mediante un PIN. Posteriormente, si por ejemplo esta compra se ha hecho asociando un número de tarjeta Visa, la transacción se llevará a cabo a través de la red VisaNet y será esta la encargada de comunicar la entidad financiera del cliente con la del comercio.

Este sistema de pago es muy rápido seguro y cómodo, pero cuenta con un grave problema de estandarización. Según un estudio realizado por la empresa Mobile Distillery, para poder cubrir un 30% del mercado de usuarios móviles es necesario ofrecer soporte para más de 150 modelos de teléfonos diferentes, lo cual puede suponer un problema.

Aun así, gracias a la comodidad que aporta, la fácil usabilidad por parte de los usuarios y el interés que están demostrando tanto entidades financieras como compañías vinculadas al mundo de las telecomunicaciones para que esta plataforma de pago salga adelante, parece que el NFC va a ser la tecnología definitiva que consagre los pagos mediante terminal móvil.

Actualmente una de las grandes compañías que ha apostado por esta tecnología de pago con móvil es Google, con la aplicación Google Wallet, la cual se empezó a utilizar en EE.UU y solo permitía la vinculación de tarjetas de crédito MasterCard y actualmente Visa ya se encuentra unida a este sistema de pago del cual se puede disfrutar ya en multitud de países por todo el mundo, entre ellos España.

8.- CASOS DE ÉXITO

En este capítulos se expondrán algunos de los casos de éxito llevados a cabo para realizar pagos mediante terminal móvil.

8.1.-NFC en Sitges

En el año 2010 los habitantes de Sitges, un pueblo costero de la provincia de Barcelona pudieron disfrutar de una campaña denominada Mobile Shopping Sitges gracias a la colaboración de las empresas Telefónica, Visa y La Caixa.

Esta campaña consistía en un proyecto piloto que trataba de incentivar el pago con móvil entre los 1500 habitantes de Sitges. Para ello todos los habitantes de esa localidad que fuesen clientes de Telefónica y La Caixa podían optar gratuitamente a un teléfono Samsung Star S5230 con tecnología NFC, en el que se insertaba una tarjeta SIM de Visa en la que se almacenaban los medios de pago. Por otro lado unos 500 comercios disponían de TPV con función NFC para permitir los pagos con móvil.

Este proyecto piloto duró medio año y los resultados fueron todo un éxito. El 90% de los clientes pagaron con móvil y el 80% de los comercios que participaron realizaron transacciones utilizando el sistema habilitado para la ocasión.

Como datos curiosos destacar que el 60% de las ventas no superaron los 20€, y que se produjeron en su mayoría entre semana en bares, restaurantes y supermercados. En una encuesta realizada a los usuarios que utilizaron el servicio le otorgaron al pago con móvil una puntuación de 8 sobre 10 y declararon que les parecía un método rápido fiable y sencillo. La media de edad de los usuarios era de 46 años y el 90% de ellos declaró la intención de seguir utilizando ese método de pago aun acabando el

proyecto piloto por lo que tanto Telefónica como La Caixa decidieron dejar activo el servicio de forma indefinida.

Hay que decir que en términos de seguridad, al ser un proyecto participado activamente por Visa, los pagos estaban autenticados por 3D-Secure, lo cual como se ha visto en capítulos anteriores permite autenticar de una manera muy segura a todos los titulares de las tarjetas implicadas en una transacción. Hay que decir que no todos los sistemas de pago implementados, independientemente de la tecnología, permiten la compatibilidad con 3D-Secure, lo cual es un extra a favor en términos de seguridad.

8.2.-Pagos con móvil en la EMT de Madrid

El año pasado la operadora móvil virtual de Bankinter y la empresa municipal de transportes EMT llegaron a un acuerdo para poder habilitar el pago del transporte móvil mediante móviles con tecnología NFC.

Para esta experiencia piloto se seleccionó a un grupo de personas que eran usuarios del servicio de telefonía de la operadora móvil de Bankinter.

Nuevamente en este sistema de pago NFC la tarjeta SIM incorpora la aplicación capaz de gestionar los títulos de transporte reconocidos al acercar el teléfono a una máquina validadora con tecnología NFC.

Además este sistema permite al usuario adquirir nuevos títulos y recargas de transporte a través de la web o de su teléfono móvil.

Como novedad, la empresa Ericsson ha participado en la experiencia aportando un sistema de seguridad para la comunicación NFC que tiene lugar entre los proveedores de servicios NFC, en este caso la EMT, y los operadores móviles. El sistema se denomina TSM (Trusted Service Manager) en a grandes rasgos su función es permitir un acceso seguro a la tarjeta SIM del móvil.

En cuanto a lo que se refiere al funcionamiento, este tipo de aplicaciones funcionan de diferente manera a las aplicaciones desarrolladas para el pago en un comercio. En este caso el dispositivo NFC del que se dispone en el autobús o en la marquesina no es el encargado de realizar la comunicación con la entidad bancaria para la transacción, sino que a través de la comunicación que se produce con el terminal móvil deduce del título del abono que lleva el usuario en el móvil la cantidad pertinente.

Para este tipo de usos la tecnología NFC es muy apropiada y aporta una seguridad más que suficiente para que los usuarios puedan optar por ella sin ningún tipo de recelo en este sentido.

8.3.-Pago por móvil en la EMT de Málaga

La EMT de Málaga también inició un proyecto piloto para efectuar los pagos de autobús público mediante terminal móvil. Este proyecto es anterior al de la EMT de Madrid.

En este proyecto participaron las empresas Orange e Indra para desplegar una plataforma de pago NFC a bordo de los autobuses de Málaga.

En este caso también se utiliza una tarjeta SIM adaptada que permite al usuario hacer uso de la tecnología NFC.

Para la prueba piloto se contó con 150 usuarios que incorporaban en su terminal móvil una aplicación denominada Cartera Orange que le permitía al usuario poder comprar su título de viaje en cualquier momento y validar cada viaje en el momento de subir al autobús, únicamente con el gesto de acercar el teléfono al lector situado dentro del vehículo. La aplicación también le permite al usuario llevar un historial de los viajes realizados y de los gastos acumulados.

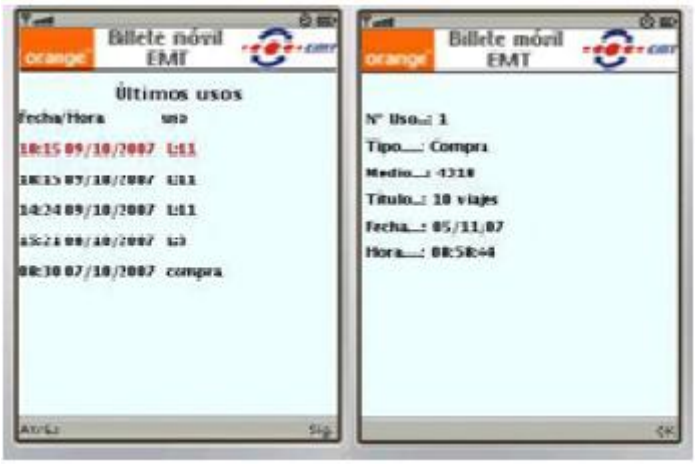

Figura 8.1

Para este proyecto la EMT de Málaga también desplegó en las marquesinas de las paradas de autobuses unas etiquetas que permitían al usuario consultar el tiempo real con simplemente acercar el terminal móvil.

8.4.-Pagos a través de iPhone en Starbucks

La cadena Starbucks está realizando una prueba piloto en Estados Unidos que permite a los clientes utilizar una aplicación dedicada para pagar sus compras mediante el iPhone.

La cadena pretende así habilitar un modo de pago específico para los productos que se puedan adquirir en sus establecimientos, tales como, cafés, batidos, bollos, pasteles, etc. De modo que puedan ser pagados en este caso mediante una aplicación específica desarrollada para iPhone.

Starbucks ha iniciado este proyecto piloto en unas 1000 de sus tiendas en la ciudad de Seattle y en el norte de California.

La experiencia por el momento está resultando ser un éxito por lo que la compañía piensa en expandir la experiencia a más sedes.

La aplicación de pago Starbucks está disponible de forma gratuita en el App Store de Apple y permite a los usuarios asociar el pago a una tarjeta de crédito propia para disponer de saldo. Mediante la aplicación el usuario elige el producto y muestra el código de barras que le sale en pantalla para que pueda ser leído por un lector de código de barras. Una vez que el lector de barras realiza la lectura y confirma la transacción de compra, la aplicación realiza del descuento necesario en la tarjeta asociada del cliente.

En este caso el TPV tampoco es el encargado de realizar la transacción, sino que es la aplicación a través de sus servidores quien da la autorización para poder realizar el pago desde las tarjetas de crédito asociadas a la aplicación de pago.

Desde el punto de vista de seguridad, todos los datos bancarios del usuario están disponibles dentro de servidores de Apple, y la comunicación con las diferentes instituciones bancarias se realiza mediantes redes privadas o VPNs, sin necesidad de que el usuario tenga que facilitar esos datos desde su terminal pudiendo suponer una amenaza de seguridad.

Figura 8.2

8.5.-Sistema NFC desplegado por Visa para los Juegos Olímpicos

Visa presentó durante el Mobile World Congress de Barcelona de este año, todo un catálogo de aplicaciones y dispositivos equipados con sistema NFC que desplegará para los Juegos Olímpicos.

Visa podrá desplegar esta infraestructura de pago gracias al acuerdo alcanzado con el banco Lloyds y la operadora móvil O2.

Con este sistema se podrá pagar el autobús o realizar pequeñas compras en los aledaños de la Villa Olímpica. Para transacciones de más 20€ se solicitará al usuario la introducción de un código de uso para esa aplicación que es diferente del PIN de la tarjeta.

También existe la posibilidad de acuerdo con la compañía Vodafone para poder llevar a cabo un sistema de pago basado en una aplicación e-wallet de cuyo desarrollo se encargaría el fabricante de sistemas de pago para certificar su seguridad.

En un evento tan grande las posibilidades de robo o pérdida se multiplican, pero los usuarios pueden estar tranquilo porque la información bancaria irá encriptada dentro de la tarjeta SIM, por lo que solo será posible acceder a ella conociendo el PIN. Además bastará con avisar de la pérdida al banco o al operador para que se cancelen las futuras transacciones

Figura 8.3

Además, en cuanto a seguridad hay que tener en cuenta que los pagos mayores de 20€ serán validados mediante el protocolo 3D-Secure al ser un sistema desarrollado por Visa. Por lo que los usuarios tienen un plus de confianza a la hora de poder optar por este sistema debido al complejo y más que seguro sistema de autenticación de titulares de las tarjetas.

9.- FUTURO DE LOS PAGOS CON MÓVIL

Los pagos con móvil están evolucionando mucho y todo apunta a que será un método de pago que se adoptará de forma masiva por parte de los usuarios en los próximos años, ya que parece ser la que más agrada a los usuarios por su simplicidad, rapidez y seguridad.

Pero sin embargo, de momento no ha gozado de toda la aceptación que se esperaba. Todas las previsiones hechas por los expertos apuntaban que en el año 2012 el pago con móvil se adoptaría masivamente, y de momento no ha sido así.

Son muchos los factores que influyen para que los sistemas de pago con móvil sean aceptados de manera global por parte de los usuarios. Por un lado están los problemas de estandarización, ya que al no haber una plataforma estandarizada que permita realizar los pagos con móvil limita mucho la usabilidad por parte de los clientes y por otro lado incrementa mucho la inversión que tiene que hacer una empresa para poder desplegar una plataforma de pago.

Por otro lado se encuentran las reticencias que muestran algunos usuarios respecto a la seguridad de los pagos con móvil, ya que según encuestas realizadas sobre el tema (EuropaPress) reflejan que un 30% de los encuestados muestran su preocupación respecto al manejo de la información financiera personal durante las transacciones móviles.

Seguramente la mayor barrera que se está topando la expansión de los pagos con móvil es el conflicto que mantienen las partes implicadas en la solución para verse beneficiadas. En este punto las operadoras móviles juegan un papel muy importante dentro de la solución y quieren que esa importancia se vea reflejada en el pago en forma de comisiones, y no siempre consiguen a llegar a acuerdos con las entidades financieras.

Además esto obliga por otra parte a contemplar un nuevo marco legal por definir donde habría que incluir a las operadoras móviles.

No obstante, hay que decir que el papel de las operadoras móviles, más allá de lo puramente técnico, puede ser decisivo en muchos escenarios. Por ejemplo en países subdesarrollados donde la población no tiene los recursos suficientes como para que un banco le pueda facilitar una tarjeta de crédito, pero sin embargo sí pueden acceder fácilmente a tener un teléfono móvil, las operadoras móviles son un recurso muy valioso para que este tipo de población pueda realizar los pagos con móvil.

Son modelos no basados en bancos, donde Los clientes no tienen ninguna relación contractual directa con ninguna institución financiera sujeta a reglamentación y pueden realizar sus transacciones en establecimientos de comercio minorista que hacen las veces de agente para la prestación de estos servicios, y el "dinero" del cliente se registra en una cuenta virtual en el servidor de la operadora móvil.

Estos modelos también permiten que los clientes puedan realizar transacciones de pago y de transferencia de fondos entre los usuarios del mismo sistema, así como transferir dinero de una cuenta a otra y pagar sus facturas.

Como he dicho estos sistemas de pago tienen mucho éxito en países en vías de desarrollo donde normalmente la población no tiene acceso a cuentas bancarias ni tarjetas de crédito.

Pero sin embargo, también en los países desarrollados las operadoras móviles quieren adquirir funciones de entidad financiera, para que el usuario pueda adquirir un producto y el importe sea cargado directamente en su factura mensual de teléfono sin necesidad de que haya una entidad financiera de por medio.

El caso más reciente es el de Telefónica, que ha llegado a un acuerdo con las grandes empresas del sector para que los usuarios puedan adquirir cualquier aplicación o juego sin necesidad de teclear el número de su tarjeta de crédito, y que lo carguen a final de mes en la factura.

Telefónica ya ha comenzado a ofrecer estos servicios en Alemania y tiene previsto incorporarlo a 14 de sus negocios operativos en todo el mundo de aquí a final de año, incluyendo países como España, Reino Unido y Brasil.

A pesar de todos los inconvenientes que pueda presentar actualmente el pago con móvil, y las trabas que hemos señalado, todos los datos apuntan a que el pago con terminal móvil se acabará consolidando como forma de pago.

Cada día hay más consumidores que optan por el m-commerce. Los datos de la empresa Nielsen señalan que un 60% de los propietarios de smartphones en EEUU lo han usado en alguna compra. Por otro lado, IBM ha realizado un estudio donde que casi un 20% de las compras online de minoristas en EEUU, se iniciaron a finales de 2011 desde un dispositivo móvil (cuando en 2010 esta cifra fue del 8,4%).

Las previsiones para el comercio móvil son muy buenas: Forrester calcula que los beneficios se triplicaran en los próximos 4 años

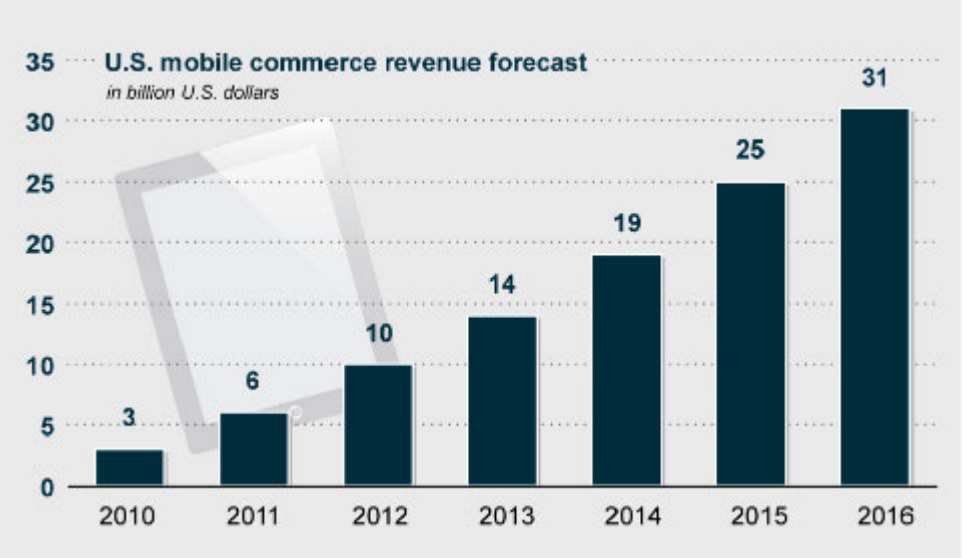

Figura 8.4

Aquí en España hoy en día uno de cada cinco teléfonos móviles es compatible con la tecnología NFC. Y para seguir fomentando la utilización de esta tecnología los principales operadores han suscrito un acuerdo para favorecer la implantación de NFC, y se calcula que a mediados de 2013, al menos un 30% de los teléfonos móviles estarán dotados de esta característica.

Un factor que en España puede retardar la implantación definitiva de los pagos con móvil como una opción cotidiana, es el papel de las entidades financieras, ya que juegan un papel fundamental a la hora de poder desarrollar este sistema de pago y en España están atravesando por un momento muy difícil debido a la situación económica, por lo que quizás no sea el mejor momento para embarcarse y apostar por una nueva forma de pago. En este sentido la consecuencia más directa para los consumidores serían son las comisiones que hoy en día oscilan entre el 1% y el 6%.

10.-CONCLUSIONES

Todo parece indicar que más pronto que tarde los pagos con móvil serán una realidad en nuestra vida cotidiana. A pesar de todas las dificultades que se está topando esta nueva forma de pago, considero que las ventajas que puede aportar a la sociedad acabarán venciendo a esas dificultades.

La tecnología que parece apuntalar y lanzar definitivamente esta forma de pago es la tecnología NFC. Se trata de una tecnología que ya está madurada y ha sido probada en varios proyectos, y no solo relacionados con los sistemas de pago móvil. Además es una tecnología que reúne todos los requisitos para que el pago con móvil pueda triunfar, es segura, rápida y muy cómoda, y además a los usuarios les recuerda a la forma de pagar con la tarjeta, ya que necesitan realizar una conexión aunque sea sin cables con el TPV del comerciante.

Por otro lado, el esfuerzo que están haciendo las operadoras móviles porque este sistema de pago sea una alternativa real, hace pensar que finalmente esta forma de pago acabará implantándose. Asimismo me parecen muy interesantes las alternativas que ya están ofreciendo las operadoras móviles en los países en vías de desarrollo de poder cargar los gastos de las compras efectuadas con el móvil en la factura mensual de teléfono. En España la empresa Telefónica ya está promocionando esta práctica para poder adquirir contenido digitales y multimedia siendo el coste de estos asociados a la factura mensual de la compañía.

Este puede ser un factor que impulse el pago con móvil, ya que no obliga al usuario a tener una vinculación con una entidad bancaria, y se evita el posible miedo a que sus datos bancarios puedan ser robados o alterados.

Pero sin embargo, uno de los obstáculos que todavía puede retardar la adopción del pago mediante móvil como un método habitual, es que todavía no existe una plataforma estándar para realizar estos pagos. Es ahí

donde todavía las compañías móviles, las entidades financieras y las compañías fabricantes de terminales móviles, tienen que hacer un esfuerzo por ponerse de acuerdo y definir un estándar que facilite las cosas y permita una fácil implantación del sistema para las empresas y una fácil adquisición e interacción a los usuarios.

Finalmente, el veredicto final que dictará sentencia sobre si los pagos con móvil se acabaran implantando como una solución habitual, es la sentencia que dictaran los usuarios. Los usuarios son los verdaderos medidores de si una tecnología puede triunfar o no. Muchas veces a pesar de los esfuerzos de las compañía por intentar introducir una nueva tecnología que está más que madurada fracasan porque los usuarios no le dan su aprobación. Ya sea por desconfianza o porque no la consideran necesaria o porque no se adapta a los estándares sociológicos del momento.

Pero personalmente no creo que este sea el caso. En España el éxito del que gozan los terminales móviles es muy alto, más aún con los de última generación (smartphones), y por otro lado los sistemas de pago electrónicos, sobre todo con tarjetas de crédito, están de sobra aceptados y son usados cotidianamente, por lo que la combinación de móvil y sistema de pago acabará resultando atractiva y práctica al usuario.

GLOSARIO

MS: Estación móvil
SIM : Modulo de identificación de abonado.
IMSI: Identificación internacional de abonado móvil
TMSI: Identificación temporal del abonado móvil.
PIN: Número de identificación personal.
PUK: Clave personal de desbloqueo.
GSM: Sistema móvil global.
GPRS: Sistema global de paquetes en la red radio.
NIP: Número de identificación personal
TPV: Terminal punto de venta.
SMS: Servicio de mensaje cortos
USSD: Servicio de datos suplementario no estructurado.
PAN: Red de área personal.
WAP: Protocolo de aplicación inalámbrica.
NFC: Campo de contacto cercano.
P.O.S: Punto de venta.
ACS: Servidor de control de acceso.
CAVV: Valor criptográfico llamado valor de verificación de autenticación
AHS: Servidor histórico de autenticación.
ECI: Identificador de comercio electrónico
SSL: Capa de conexión segura.
SET: Transacción electrónica segura.

BIBLIOGRAFÍA

[1] Maryam Asadi Tehrani, Ali Asghar Amidian, Jafar Muhammadi, HamidReza RabieeA. "survey of system platforms for mobile payment". 2010 International Conference on Management of e-Commerce and e-Government IEEE.

[2] Nts-solucions. "Estudio de plataformas de pago por movil". Estudio realizado para la dirección de innovacion y administración electrónca del Gobierno Vasco. 2010.

[3] Justo Carracedo Gallardo. Seguridad en redes telematicas. Editorial McGraw-Hill. Año 2004.

[4] Ana Gómez Oliva. Transparencias de la asignatura impartida en master "Servicios telemáticos para la sociedad de la información". Tema 3. 2010-2011

[5] A.Sarajlic, D,Omerasevic. Access channel in m-commerce services. Proceeding of the ITI 29th conference on information technology interface, Cavtat, Croatia , June 25-28 2007.

[6] Ashok Goudar, Mobile Transactions and Payment Processing. 2011

[7] Mahil Carr, Mobile Payment Systems and Services. 2010

[8] CMT, Informe sobre el comercio electrónico. 2012

[9] Milena Head & Eldon Y. LI, Mobile and Ubiquitous commerce, 2010

[11] https://itunews.itu.int/es/1725-Banca-movil.note.aspx

[12] http://blogcmt.com/2012/04/24/el-peso-del-m-commerce

[13] https://cms.paypal.com/es/cgi-bin

[14] http://windowsphoneapps.es/tutorial-ayuda/nfc

[16] *http://www.dat.etsit.upm.es/~mmonjas/pago/protocolos.html*

[17] *Arnulfo Castro Vásquez, Estándares de métodos de pago por móvil. 2011*